TREADSTONE 71 ADVERSARY INDEX

# The Treadstone 71 Adversary Index

## Tier 0 Free Edition · Q3 2026

Big Four in depth across three tearlines, with the 42-actor field at catalog level

Issue date: October 5, 2026 · Horizon through January 15, 2027

**China 89 · Russia 85 · DPRK 79 · Iran 77**

Tier 0 Free Edition · v1.1 · the free public report · standard weighting: each composite equals the rounded mean of eight sub-indices

| Document control | |
|---|---|
| Edition | Tier 0 Free Edition, Q3 2026, version 1.1 |
| Issue date | October 5, 2026 |
| Evidence cutoff | October 4, 2026 |
| Scoring window | May 15 to September 28, 2026 |
| Next release | January 15, 2027 |
| Composites | China 89, Russia 85, DPRK 79, Iran 77. Iran rose one point from 76. |
| Publisher | Treadstone 71 LLC, Half Moon Bay, California. treadstone71.com |

Copyright 2026 Treadstone 71 LLC. All rights reserved. Read this edition, share it in full and unaltered, and cite it. Other uses need written permission.

## Aggregate Read: All Four

**TL;DR.** Four state adversaries lead the field. China holds 89 and Russia 85 in the top tier. North Korea at 79 and Iran at 77 sit a step below, inside Tier 1. China alone stands clear of a tier line. Russia, North Korea, and Iran sit inside the review band of 75 to 85 and carry a standing senior-analyst review. The scores hold the quarter (Likely, 55 to <85 percent). Each adversary runs reinforcing operations against a different center of gravity: China against the United States (US) and its Indo-Pacific allies, Russia against NATO Europe and Western lifeline sectors, North Korea against the cryptocurrency sector that funds the regime, and Iran against the kinetic cycle in the Middle East.

One pattern repeats across the four: the score holds until quiet activity turns into a real effect.

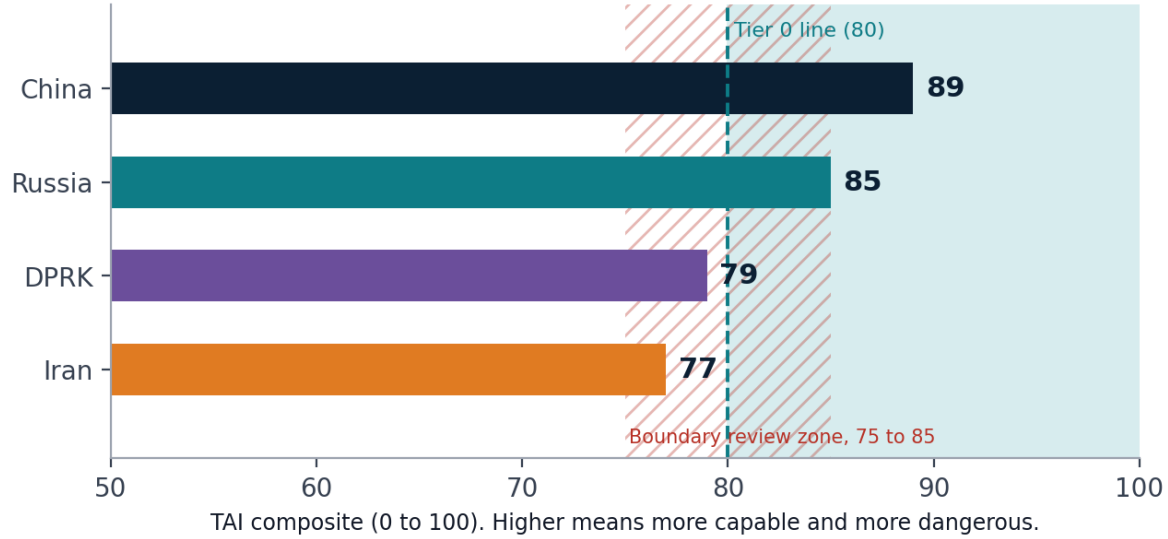



Figure 1. The Big Four composites with the tier-band backdrop and the Tier 0 line. China alone clears a tier boundary. Russia, the Democratic People's Republic of Korea (DPRK), and Iran sit inside the 75 to 85 review zone.

China ranks first at 89. Russia ranks second at 85, North Korea third at 79, and Iran fourth at 77. A firm gets pulled in through its sector, its region, or a single dependency, such as a carrier link, a remote-hire pipeline, or an exposed control system. No quarrel with a capital is required. The China-nexus loss is collection; the North Korean loss is theft. Russian and Iranian lines add disruption against lifeline and operational-technology targets.

### *Movers, Quarter Over Quarter*

Iran moved up one point, from 76 to 77. China, Russia, and North Korea held. Three documented developments carry the Iran move: Iranian state propaganda offices ran influence operations on artificial intelligence (AI) tools, the Iranian armed forces began a command restructuring on August 10, and Iranian-affiliated actors widened their exploitation of exposed industrial controllers. The gain is real but small. Counter-evidence tempers it. Three governments exposed Iranian state spyware in one advisory, and that exposure argues against credit for evasion. The Iran chapter weighs the evidence on each side.

One more change touches every actor. Standard weighting now reads on the page. Each composite equals the rounded mean of its eight sub-indices, and the sub-index tables in the Standard Weighting section reconcile all four composites to the unrounded mean.

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

| Adversary | Composite | Tier | Reading |
|---|---|---|---|
| China | 89 | Tier 0 | Catalog lead. Outside the boundary review zone. |
| Russia | 85 | Tier 0 | Inside the 75 to 85 boundary review zone. Senior-analyst review at the tier line. |
| North Korea (DPRK) | 79 | Tier 1, upper | Inside the review zone. Senior-analyst review at the tier line. |
| Iran | 77 | Tier 1 | Up one point from 76. Inside the review zone. Senior-analyst review at the tier line. |

Table 1. The field at a glance.

### *Bottom Line Up Front*

**Who.** Treadstone 71 scores 42 named adversaries on a 0 to 100 composite. The Big Four sovereign powers lead the catalog and receive full treatment here.

**What.** China 89, Russia 85, the DPRK 79, and Iran 77. Each score is the rounded mean of eight sub-indices. Iran rose one point. The other three held.

**So what.** A score near a tier line moves a budget decision. Russia at 85, the DPRK at 79, and Iran at 77 sit inside the review zone, so a firm should treat each as live and re-read it at the January 15, 2027, release.

**Why now.** The Q3 window opened about five months after the death of Supreme Leader Ali Khamenei on February 28, 2026, with his son Mojtaba Khamenei in office since March 8. Two multinational advisories closed it in one week, one on Iranian spyware (September 15) and one on North Korean developer targeting (September 18). A Russian influence push aimed at the November 3 US midterms ran alongside.

**Impacts so far.** Iranian AI-assisted influence is documented at the state-office level. North Korea ran its theft and hiring schemes at scale. Russia drew little audience for its midterm content while its espionage tempo held. China relied on influence and AI operations that platform researchers documented, and government advisories on Chinese operations stayed absent from the window.

**Outlook.** All four scores hold through January 15, 2027 (Likely, 55 to <85 percent). Russia-linked operations will likely keep releasing fake-branded midterm content through November 3, 2026. A single item reaching a mass organic audience is unlikely (15 to <45 percent). An FBI statement naming North Korea for the September 24 Bitget theft before January 15, 2027, stands at roughly even chance (45 to <55 percent).

**Recommendations.** Fund edge-device and identity hardening first, because one program answers Chinese and Russian intrusion that breaks in through the same equipment. Screen remote hires and suppliers next, then protect cryptocurrency custody and communications. Assign one named observable per adversary to a watch owner so posture moves on a signal and not on a headline.

**Opportunities.** A board gains one scored axis for resource allocation in place of vendor catalogs that resist comparison. Convergence coverage lets one hardening spend answer more than one state. A named observable per adversary turns escalation into a mechanical decision.

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

## How to Read the Edition

The edition runs in four labeled tearlines, split by audience and not by classification. Strategic speaks to the board and the C-suite. Risk, governance, security leadership, and the intelligence function read the Operational tearline. Analysts, hunters, and collection managers read the Tactical tearline, which holds operator behavior and tradecraft. Detection engineers and the security operations center read the Technical tearline, which holds machine artifacts. All four composites read identically across the four. A reader descends as far as the role asks and no farther. Inside each tearline the four adversaries appear in composite order: China, Russia, the DPRK, and Iran.

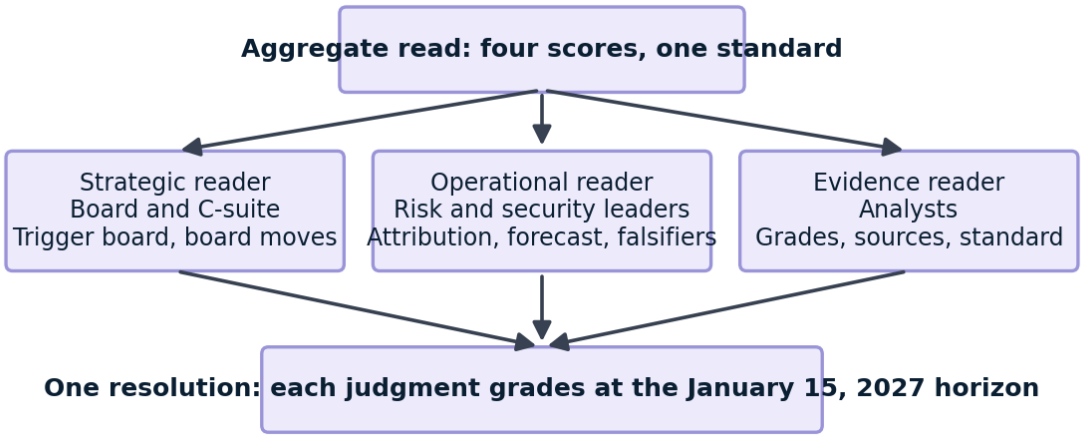



Figure 2. Whole-report flow. Same findings, three reader paths, one resolution.

Two legends carry the language. Probability terms follow Sherman Kent, with half-open bands. Evidence grades follow the NATO Admiralty Code: a letter for source reliability (A to F) and a digit for information credibility (1 to 6). The two grades stay separate and never average. A grade such as B2 reads usually reliable, probably true. Every development in the edition carries one of three labels. A verified record comes from an official or primary document. Researchers or the press supply a third-party attribution. Adversary claims come from the actor or its own media. The labels never share a sentence. Grades never average.

| Likelihood term | Interval, percent | Use in the edition |
|---|---|---|
| Almost certain | 95 to 99 | Reserved for confirmed or structural facts |
| Highly likely | 85 to <95 | Strong judgment with corroborated sourcing |
| Likely | 55 to <85 | Default for score holds and base-case forecasts |
| Roughly even chance | 45 to <55 | Used where evidence splits |
| Unlikely | 15 to <45 | Alternative outcomes |
| Highly unlikely | 5 to <15 | Tail outcomes |
| Almost no chance | 1 to <5 | Excluded from planning |

Table 2. Likelihood terms and bands.

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

### *What the Index Scopes In and Leaves Out*

A reader who knows the edges of the product reads it better. Three boundaries shape what the index delivers.

**No dollar figure, on purpose.** A credible loss number rests on facts the index does not hold: the reader's revenue, the cost of an hour of downtime, the value of the reader's crown jewels, and the maturity of the reader's controls. A figure printed without those inputs misleads. The money question moves to a per-client layer that prices impact against that client's own environment.

**No league table against peers, on purpose.** A state actor selects a target on sector, mission, and access opportunity, not on whether a competitor patched faster. Volt Typhoon does not pre-position in a network because a rival fell behind. A peer ranking invites false comfort. The useful version of the question is threat prevalence: which adversaries target the reader's sector and region, and how often.

**No indicator feed, on purpose.** The index publishes no indicators of compromise, no detection signatures, and no technique-by-technique map. Those layers sit in products the reader already buys. The index runs above them, on attribution, scoring, forecast, and decision.

## Standard Weighting: How a Composite Is Built

Every composite reads as the rounded mean of eight sub-indices. Each sub-index scores 0 to 100 and blends documented domains into one measure. Equal weight applies across the eight in the composite. Inside each sub-index, the roll-up follows a rubric whose domain weights stay with the paid editions. Eight measures, one number.

| Code | Sub-index | What it measures |
|---|---|---|
| CWV | Cognitive Warfare Velocity | Pace and reach of cognitive influence operations |
| OPS | OPSEC Sophistication | Intrusion, security, and surveillance tradecraft |
| AEI | Adaptation/Evolution Index | How fast the actor adapts under operational pressure |
| NV | Narrative Volume | Aggregate state-aligned narrative production |
| STC | Sectoral Targeting Concentration | Industry coverage, depth, and functional targeting |
| ATA | AI Tradecraft Adoption | Documented operational use of AI |
| DM | Doctrinal Maturity | Codified doctrine, training pipeline, unit permanence |
| OT | Operational Tempo | Frequency, escalation pattern, operational diversity |

Table 3. The eight sub-indices.

| Actor | CWV | OPS | AEI | NV | STC | ATA | DM | OT | Sum / mean | Composite |
|---|---|---|---|---|---|---|---|---|---|---|
| China | 92 | 92 | 82 | 90 | 88 | 88 | 89 | 88 | 709 / 88.625 | 89 |
| Russia | 88 | 85 | 78 | 89 | 80 | 82 | 90 | 87 | 679 / 84.875 | 85 |
| DPRK | 94 | 83 | 71 | 92 | 78 | 48 | 85 | 81 | 632 / 79.000 | 79 |
| Iran (Q3) | 83 | 79 | 69 | 79 | 77 | 78 | 71 | 77 | 613 / 76.625 | 77 |
| Iran (Q2) | 82 | 78 | 68 | 78 | 76 | 76 | 70 | 76 | 604 / 75.500 | 76 |

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

Table 4. Sub-index scores, sums, means, and published composites. A mean rounds half up.

| | CWV | OPS | AEI | NV | STC | ATA | DM | OT |
|---|---|---|---|---|---|---|---|---|
| China | 92 | 92 | 82 | 90 | 88 | 88 | 89 | 88 |
| Russia | 88 | 85 | 78 | 89 | 80 | 82 | 90 | 87 |
| DPRK | 94 | 83 | 71 | 92 | 78 | 48 | 85 | 81 |
| Iran (Q3) | 83 | 79 | 69 | 79 | 77 | 78 | 71 | 77 |

Figure 3. The eight sub-indices for the Big Four. Darker cells score higher. North Korea stands out for an exceptionally low AI Tradecraft Adoption score beside very high narrative and cognitive scores.

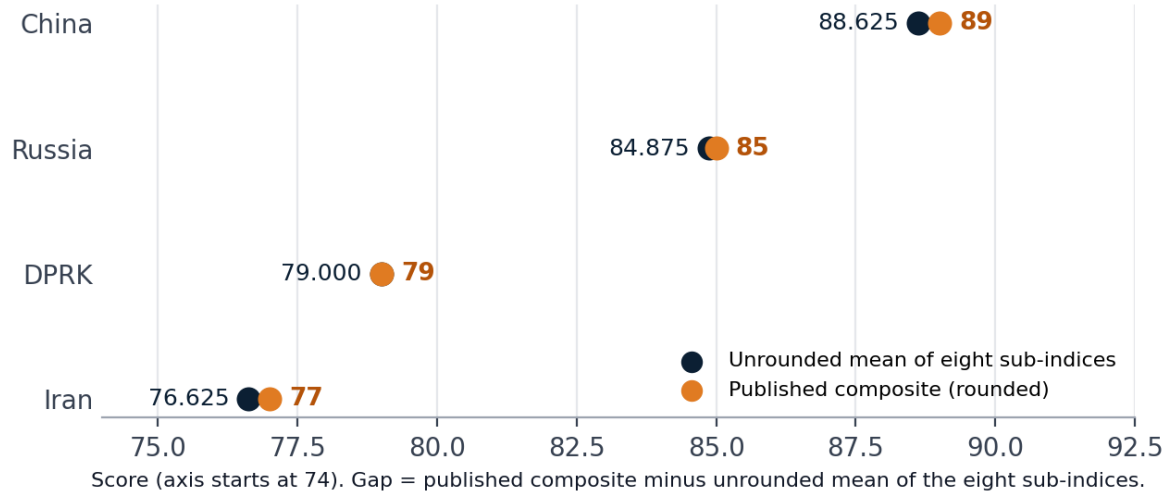



Figure 4. Reconciliation of each published composite with the unrounded mean of its eight sub-indices. Every gap is rounding alone.

The arithmetic closes. China averages 88.625 and rounds to 89. Russia averages 84.875 and rounds to 85. The DPRK averages exactly 79. Iran averages 76.625 and rounds to 77. The Iran Q2 baseline averaged 75.5 and rounded to 76 under round-half-up, so Iran moved one composite point on a gain of nine sub-index points. Rounding runs half up.

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

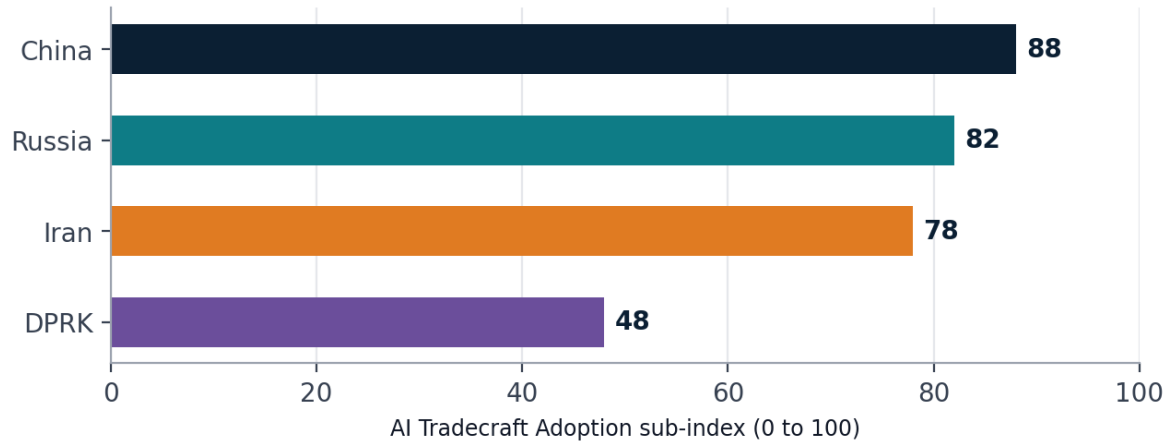



Figure 5. AI Tradecraft Adoption separates the Big Four more sharply than any other sub-index in the edition. The DPRK reads 48 against China at 88.

### *Tier Bands and Distribution*

Four bands give the composite a plain meaning. Tier 0 runs 80 to 100 and marks the peer powers. High capability fills Tier 1 at 55 to 79. Tier 2 spans 35 to 54 and marks operational capability. At 0 to 34, Tier 3 holds degraded actors, after arrest, defeat, or collapse. The 42-actor catalog splits two, nine, 27, and four across Tiers 0 to 3. Russia at 85 sits at the edge of the review zone. The DPRK at 79 and Iran at 77 sit one band down and carry the same standing review.

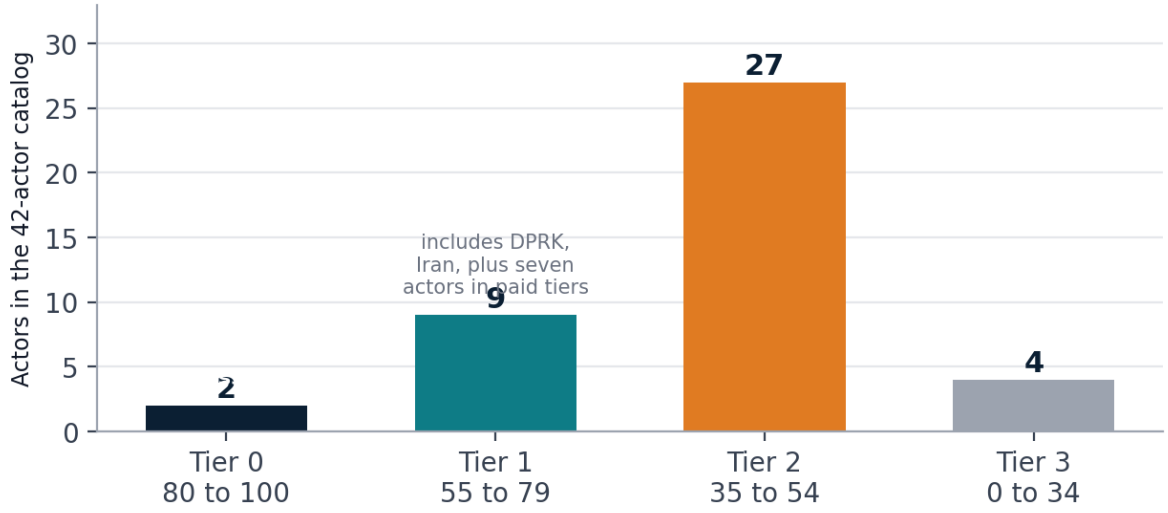



Figure 6. Tier distribution of the 42-actor catalog.

## The Q3 Evidence Window

The scoring window ran May 15 to September 28, 2026. Evidence cutoff: October 4, 2026. Treadstone 71 read government advisories first, then platform disclosures and independent research, then press reports. The record rests on 44 sources. Every address in the source list was tested on October 4, 2026, and none returned a not-found error. Five sites block scripted requests. All five open in a normal browser.

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

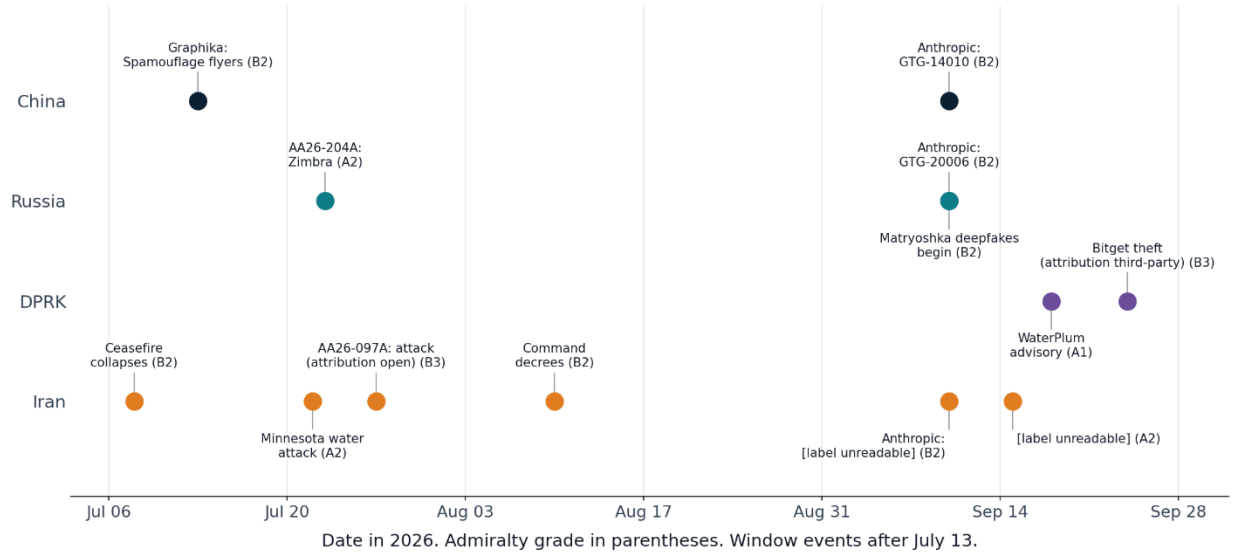



Figure 7. The Q3 evidence window by date. Colors mark the actor. Admiralty grades appear in parentheses.

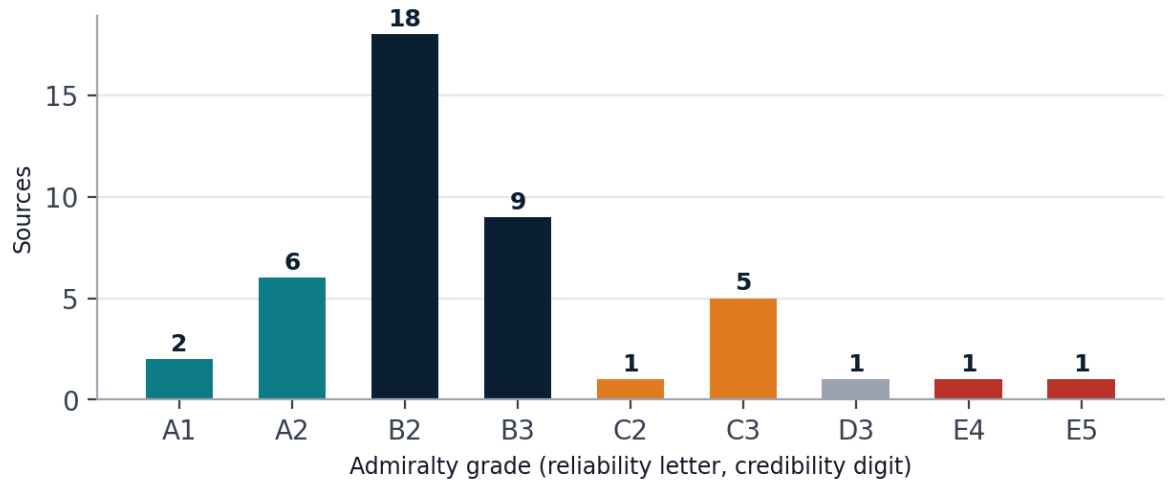



Figure 8. The 44 sources by Admiralty grade. Government records anchor the A grades. Most platform and vendor reporting sits at B2.

The window shows one pattern.

Governments published the records that carry the most weight on Iran, Russia, and North Korea.

Platform and AI-company disclosures carried the weight on China. A tier of press and state-aligned media filled the rest, and the edition marks each of those items by label and grade. The sections below take the four actors in composite order.

## Tearline 1: Strategic, for the Board and the C-Suite

### *If You Read Nothing Else*

Five steps convert the edition into a decision. A board reads the steps and stops. The operational reader runs them.

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

1. **Know your sector and region.** The index selects a firm based on its operations and footprint, not on any quarrel with the adversary. Name your lifeline exposure, your data holdings, your payment exposure, and your footprint.
2. **Run the selection function.** For each adversary, read the IF table in the Operational tearline. Where a condition matches your firm, that adversary selects you and the matching line is live.
3. **Fund the converged controls in order.** Lead with edge-device and identity hardening. One spend answers Chinese and Russian state intrusion that enters through the same equipment. Then screen insiders and remote hires, isolate operational technology, and test restores.
4. **Set the four observables as board triggers.** Assign each adversary's one observable to a watch owner. Posture moves on a named signal, not on a headline.
5. **Resolve at January 15, 2027.** Each prediction enters the record at issue and grades at the next release. The verification record makes the check mechanical.

The score runs 0 to 100. Higher means more capable and more dangerous. Tier 0 starts at 80, the peer-state threats. Tier 1 covers 55 to 79. The Q3 forecast issues October 5, 2026, and resolves at the January 15, 2027 horizon.

### *Portfolio Trigger Board*

| Adversary | Today | The one observable | If it does not fire | If it fires |
|---|---|---|---|---|
| China 89 | Tier 0 lead, holds | Access-holding turns to a disruptive effect in a US lifeline sector, or a Taiwan exercise pairs with cyber effect | Score holds. Espionage and pre-positioning dominate. | Read shifts from collection to coercion |
| Russia 85 | Tier 0, boundary zone | Quiet access turns to a disruptive effect in a Western lifeline sector | Score holds. Espionage and positioning dominate. | Score moves toward the boundary. Activate destructive-incident playbooks. |
| DPRK 79 | Tier 1 upper, boundary zone | Revenue theft turns toward a destructive effect, or a capability jump arrives through the Russia partnership | Score holds. The revenue engine runs at tempo. | Threat shifts from financial to strategic. Re-score toward the Tier 0 line. |
| Iran 77 | Tier 1, boundary zone, up one point; war in its eighth month | Renewed large-scale US strikes on Iran, floated for after the November 3 midterms | Score holds. The stalemate of blockade, Hormuz friction, and episodic strikes continues. | The disruptive operational-technology line rises within days, as it did after the July 8 collapse. Activate OT-incident playbooks. |

Table 5. Portfolio trigger board.

### *China: The Strategic Read*

**TL;DR.** China is the catalog lead at 89, the one Big Four actor clear of a tier line. The Ministry of State Security (MSS) and the People's Liberation Army (PLA) press the United States and its Indo-Pacific allies through three operations that reinforce one another: pre-positioning inside lifeline infrastructure, backbone espionage, and AI-augmented influence. Base case: 89 through January 15, 2027 (Likely). Only one signal changes the read: access-holding that turns into a disruptive effect in a US lifeline sector, or a Taiwan exercise paired with a cyber effect. Q3 evidence shows no such turn.

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

Energy, communications, transport, water, the technology and semiconductor base, logistics, and finance each sit on a China targeting line. The US is primary and Indo-Pacific allies are elevated. Espionage, not extortion, carries the loss: the prize is the firm's intellectual property and its communications.

No new government record on China surfaced in Q3.

Q3 added platform evidence and no new government record. Graphika documented the Spamouflage network spreading altered event flyers against gatherings of Safeguard Defenders and pro-Tibet and Uyghur groups. Anthropic described a PRC government-aligned actor that used an AI model to track, profile, and recruit Uyghurs in Syria, and left unconfirmed whether recruitment worked. The same report names Chinese-speaking operators who ran AI agent swarms against about 50 organizations. Anthropic assigns them no state label, and their hands-on intrusions focused on Chinese victims.

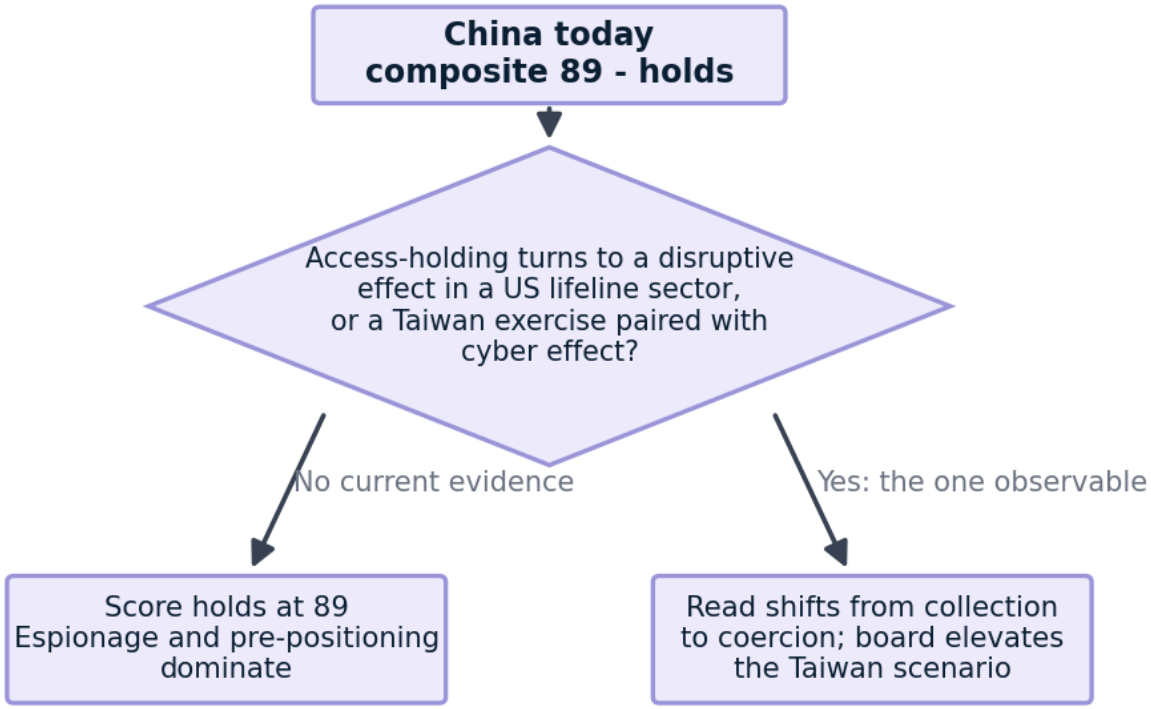



Figure 9. China: the one observable.

Over the longer horizon, what China states and what China achieves pull apart. The stated goal of national rejuvenation, unification over Taiwan, and military modernization to the 2027 benchmark rates highly likely (85 to <95 percent) as a public position and unlikely (15 to <45 percent) as a delivered outcome inside the decade. The most likely achieved path runs a protracted competition below the armed-conflict threshold: pre-positioning maintained, collection sustained at tempo, and a Taiwan status quo under rising pressure (Likely).

### *Russia: The Strategic Read*

**TL;DR.** Russia holds 85 in the top tier, inside the review zone, so the score carries a standing senior-analyst review. The Main Directorate of the General Staff (GRU), the Federal Security Service (FSB), and the Foreign Intelligence Service (SVR) press NATO Europe and the firms

inside Western lifeline sectors through three reinforcing operations: quiet intrusion through network edge devices, denial-of-service against allied government and logistics targets, and an influence push at the European governments funding Ukraine. Treadstone 71 holds 85 through January 15, 2027 (Likely). The read changes on one signal: quiet access that turns into a disruptive effect inside a Western lifeline sector. Nothing in Q3 fired it.

Russia ranks second at 85. Energy, telecommunications, transport, finance, and the defense supply base sit under pressure, with Ukraine and NATO Europe primary. A firm gets selected through its sector or footprint, not through any direct quarrel with Moscow, and a supplier inside a lifeline sector carries the same exposure as the operator it supplies.

Two Russian records led the window and pointed in opposite directions. Espionage stayed sharp. On July 23, 2026, the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency, the Federal Bureau of Investigation (FBI), and international partners issued advisory AA26-204A on a Russian state-supported group, tracked as LAUNDRY BEAR, that has exploited a Zimbra webmail flaw since at least July 2025. Influence stayed thin. Celebrity deepfakes carrying CNN branding began spreading September 10 against the November midterms, and MS NOW reported that the most popular posts drew only dozens of interactions.

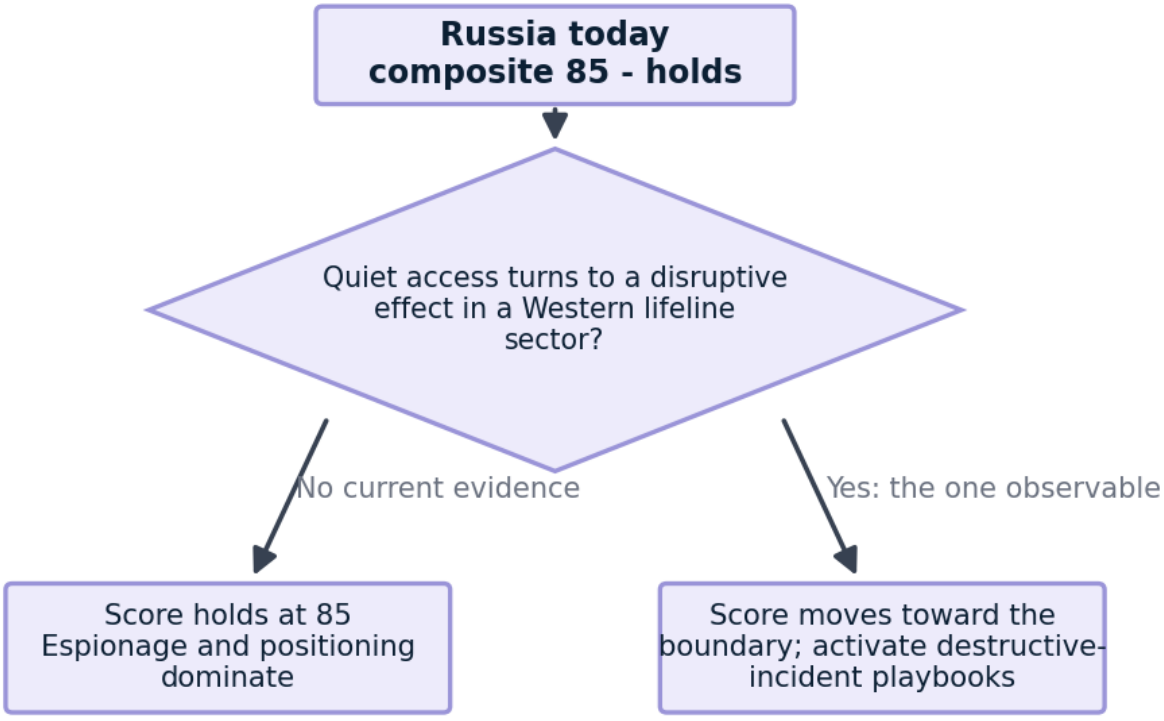



Figure 10. Russia: the one observable.

Over the longer arc, what Russia states and what Russia achieves diverge. The stated goal of a rolled-back NATO and a demilitarized Ukraine rates highly likely (85 to <95 percent) as a position and unlikely (15 to <45 percent) as an outcome. The achieved path rates a protracted, grinding conflict under sanctions strain (Likely). Q3 AI evidence argues for a higher AI Tradecraft Adoption reading than 82, and Treadstone 71 will review that sub-index at the January 15, 2027 release.

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

### *North Korea: The Strategic Read*

**TL;DR.** North Korea holds 79 at the Tier 1 upper band, in the review zone. The Reconnaissance General Bureau runs the most revenue-driven operation of the four through three lines that run together: cryptocurrency theft at state scale, fraudulent IT-worker placement inside Western firms, and espionage against defense, cryptocurrency, and blockchain targets. Expect 79 through January 15, 2027 (Likely). One signal changes the read: revenue theft that turns toward a destructive effect, or a capability jump through the Russia partnership. Q3 evidence holds no such turn.

The threat reads financial, not destructive. North Korea took 76 percent of global cryptocurrency-hack value through April 2026 and placed operatives inside more than 100 US companies, per the July 15 edition. Q3 added the strongest allied record of the window. On September 18, Japan's National Police Agency and six partner agencies published an advisory on WaterPlum, a group that lures developers with fake job interviews. The advisory counts at least 30,000 infected devices in more than 100 countries. Data from more than 7,000 cryptocurrency wallets also left in the theft, and at least 1.7 billion yen, about $10.7 million, reached wallets WaterPlum controls.

The advisory adds an organizational fact: the agencies assess that WaterPlum and some North Korean IT workers operate under the 313 General Bureau of the Munitions Industry Department. Mind the word "some." On September 24, Bitget lost about $387 million in a hot-wallet breach, and Chainalysis attributed the theft to North Korea-linked actors. No FBI statement had appeared by October 4, so the edition carries that attribution as third-party.

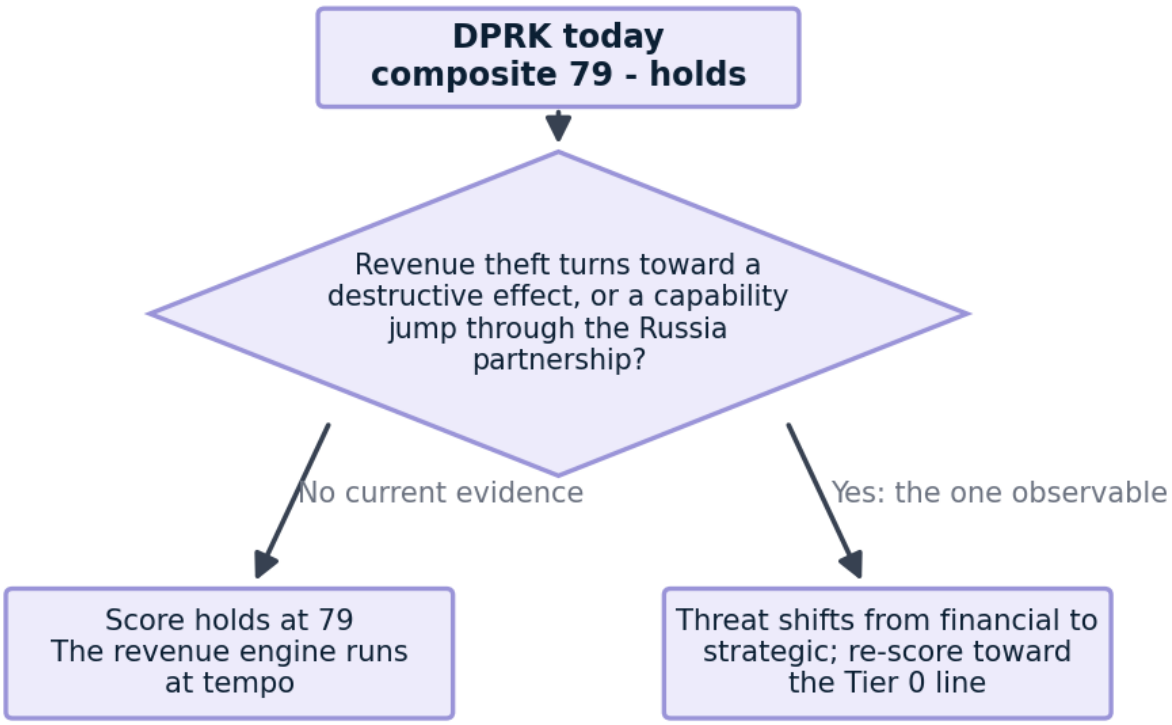



Figure 11. North Korea: the one observable.

Across the strategic horizon the triple endgame governs. The Most Likely course holds the composite in the 77 to 81 band with revenue theft sustained and the IT-worker program persistent. A shift from theft toward a destructive effect, or a capability transfer through the Russia

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

partnership, marks the Most Dangerous course. The tail runs a succession or regime shock that disrupts the operator pipeline.

### *Iran: The Strategic Read*

**TL;DR.** Iran holds 77 at the Tier 1 band, up one point, in the same review zone. The Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence and Security (MOIS) run three operational lines that rise with regional conflict: disruptive operations against operational technology, espionage and surveillance against dissidents and policy targets, and AI-augmented influence. Iran stays at 77 through January 15, 2027 (Likely). The read changes on one signal: renewed large-scale US strikes that lift the disruptive line within days. The last full exchange opened July 8 when the ceasefire collapsed. The war now runs in its eighth month, and strikes are floated for after the November 3 midterms.

Iran ranks fourth among the Big Four at 77. Water, energy, and fuel control systems, telecommunications and data holders, government and policy bodies, and conflict-exposed firms each sit on an Iran targeting line, with the US and Israel primary and Gulf hosts elevated. Iranian tempo tracks the kinetic cycle, so exposure runs episodic. Leadership is settled on paper. The Assembly of Experts named Mojtaba Khamenei Supreme Leader on March 8, 2026, and the state funeral for his father ran July 3 to 9. Consolidation of the new leadership is the central wildcard.

The war sets the clock. A Pakistani-brokered ceasefire took hold on April 8, and the United States blockaded Iranian ports on April 13. The truce collapsed on July 8, when Iranian attacks on ships off Oman drew US strikes on more than 80 targets and IRGC attacks on US bases in Kuwait and Bahrain. The blockade returned July 14. On October 1 President Trump rejected an Iranian seven-day proposal, and CNBC reported that the Wall Street Journal expects bombing to resume in November. Treadstone 71 rates renewed large-scale US strikes by January 15, 2027, as likely (55 to <85 percent), and by November 30, 2026 as a roughly even chance (45 to <55 percent).

Three Q3 developments carry the one-point rise, and one record weighs against it.

The Iran chapter of the Operational tearline lays out the record, sentence by sentence and grade by grade, so a reader evaluates each step before accepting the point.

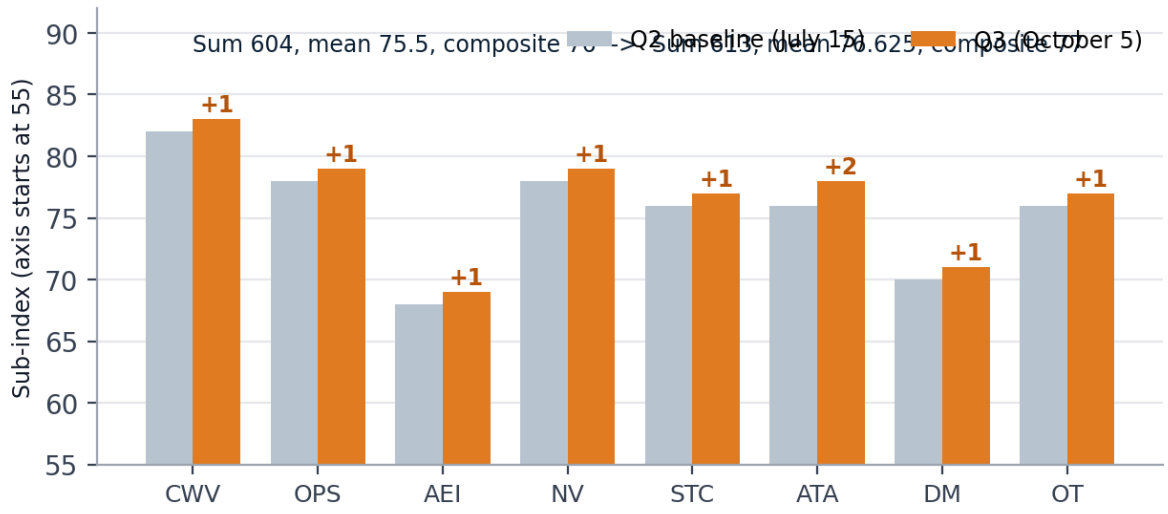



Figure 12. Iran: sub-index movement from the Q2 baseline to Q3. Nine sub-index points moved the composite one point.

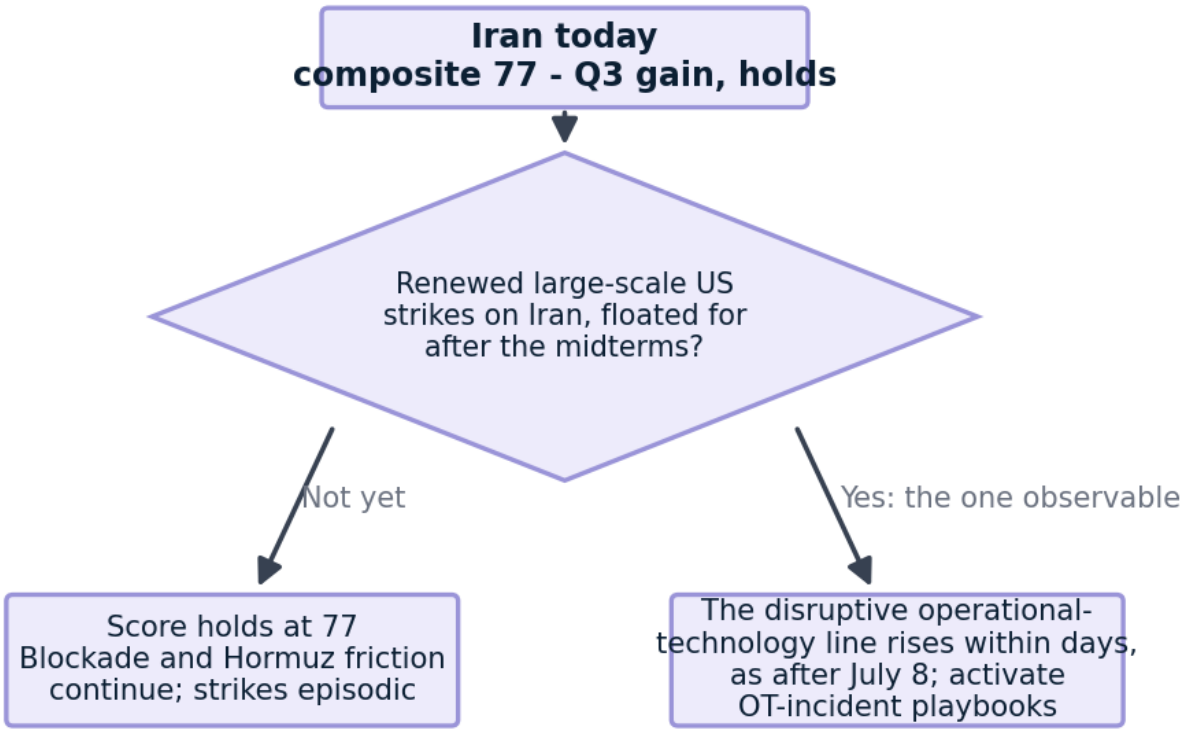



Figure 13. Iran: the one observable.

Across the strategic horizon the Most Likely course holds the composite in the 76 to 80 band with conflict-tracked spikes. A destructive operational-technology effect with physical consequence during a kinetic exchange marks the Most Dangerous course. The tail runs a succession-driven internal disruption that degrades the operator pipeline.

### *Board Moves*

Four moves carry the response.

| Board move | Why it matters | Risk it removes |
|---|---|---|
| Fund edge-device and identity hardening first | One spend answers Chinese pre-positioning and the Russian intrusion line at once, because the two enter through the same equipment | State-line initial access for a firm exposed mainly on that vector; covers two adversaries |
| Protect communications, intellectual property, and cryptocurrency custody | The China-nexus loss is collection and the North Korean loss is theft; each targets the crown jewels and the credentials | Carrier-network and intellectual-property exposure; theft of custody keys and credentials |
| Screen the remote-hire and supplier pipeline | North Korean operatives sit inside more than 100 firms; the same screening answers the Chinese insider line and the Russian supply-chain line | Insider and trusted-path routes that bypass perimeter controls |
| Set the four observables as board triggers | Each adversary carries one signal that changes its read | Over-reaction and under-reaction to headlines |

Table 6. Board moves.

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

## Tearline 2: Operational, for Risk, Governance, and the Intelligence Function

Each chapter follows one order: attribution and structure, the Q3 evidence, the selection function, and the forecast with its falsifiers. Evidence labels read verified record, third-party attribution, or adversary claim.

### *China: Operational*

The MSS and its contractor ecosystem run APT41, APT31, APT40, and APT10, while the PLA runs military cyber under the 2024 reorganization. Three lines run in parallel: pre-positioning inside US lifeline infrastructure on the Volt Typhoon pattern, backbone and technology-sector espionage on the Salt Typhoon pattern, and AI-augmented influence on the Spamouflage pattern. The first two patterns carry forward from the July 15 edition. Q3 produced new platform evidence on influence and AI, and no government advisory on Chinese state cyber operations. Court and sanctions records were not fully searched, so read that silence as a gap and not as a finding.

| Date | Development | Label | Grade | Source |
|---|---|---|---|---|
| Jul 13, 2026 | Spamouflage spreads altered event flyers through inauthentic accounts against gatherings of rights and Tibet and Uyghur groups | Third-party attribution | B2 | Graphika |
| Sep 9, 2026 | Ministry of Commerce calls the US distillation charge baseless and threatens countermeasures if Washington suppresses Chinese AI firms in its name | Verified record; claim on merits is adversary | A1 | MOFCOM |
| Sep 10, 2026 | A PRC government-aligned actor (GTG-14010) uses an AI model to track, profile, and recruit Uyghurs in Syria; recruitment success unconfirmed | Third-party attribution | B2 | Anthropic |
| Sep 10, 2026 | Chinese-speaking operators (GTG-10007) run AI agent swarms against about 50 organizations; no state label; hands-on intrusions focus on Chinese victims | Third-party attribution | B2 | Anthropic |
| Sep 10, 2026 | Seven China-based AI labs named for illicit distillation of a model; commercial extraction, not scored as state tradecraft | Third-party attribution | B2 | Anthropic |
| Sep 26, 2026 | China and the United States publish an eight-point consensus: an AI dialogue with a November round, an AI-incident channel, a bar on transit tolls on international waterways, and a military crisis-communication memorandum; no cyber point | Verified record (China's text) | A2 | MFA |

Table 7. China: Q3 evidence.

| Prediction | Most-likely line | Likelihood and grade | Competing alternative | Falsifier |
|---|---|---|---|---|
| CN-P1 Target set | Telecom and backbone operators; technology and AI firms; lifeline edge-device operators | Likely, B2 | Pivot to cloud and identity vectors | Access moves off edge devices |
| CN-P2 Verticals | Technology, telecom, government, energy, water, transport, logistics; finance elevated | Likely, B2 | Concentration narrows to technology alone | A new sector is named |
| CN-P3 Geography | US primary; Indo-Pacific allies elevated; the telecom footprint persists | Likely, B2 | Footprint contracts under hardening | No new-region telemetry by mid-horizon |
| CN-P4 Geopolitical | Collection and positioning hold; coercion stays below the armed-conflict threshold | Likely, B3 | Shift to active coercion on a Taiwan timeline | Access-to-effect transition in a lifeline sector |

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

Table 8. China: forecast and falsifiers.

| Condition (IF) | Selecting line | Example entity |
|---|---|---|
| Operates or supplies a US lifeline sector | Volt Typhoon pre-positioning | An energy, water, or transport operator |
| Depends on carrier backbones | Salt Typhoon backbone espionage | Any firm with carrier-dependent communications |
| Holds intellectual property of strategic value | MSS technology-sector collection | A semiconductor, AI, biotech, or aerospace firm |
| Is a software vendor or managed-service provider | Access-multiplier and supply-chain targeting | A managed-service, cloud, or software provider |
| Operates in or sells to Indo-Pacific allies | Regional collection and pre-positioning | A firm with Taiwan, Japan, or Philippine operations |

Table 9. China: the selection function.

### *Russia: Operational*

The GRU runs APT28, APT44 (Sandworm), Turla, and Storm-2372, and the FSB runs Energetic Bear and Gamaredon. APT29 (Midnight Blizzard) belongs to the SVR. Influence runs through Doppelganger, Storm-1516, Matryoshka, and Operation Overload. Disruption runs through NoName057(16) and its DDoSia project. Q3 evidence splits cleanly: a government advisory and an AI-company disclosure on espionage, and thin audience reach on influence.

| Date | Development | Label | Grade | Source |
|---|---|---|---|---|
| Jul 23, 2026 | CISA advisory AA26-204A: LAUNDRY BEAR (Void Blizzard) exploits Zimbra flaw CVE-2025-66376, active since at least July 2025 | Verified record | A2 | CISA |
| Sep 10, 2026 | A cluster labeled GTG-20006 uses AI agents to automate phishing and data theft and to rebuild malware after detection; more than 20 targets, mostly Ukrainian government, military, and drone supply chain. Anthropic calls the attribution consistent with public Midnight Blizzard reporting | Third-party attribution | B2 | Anthropic |
| Sep 10, 2026 | Individuals use an AI model as an editorial desk for content later published by Russian state media; Anthropic assesses the link with high confidence | Third-party attribution | B2 | Anthropic |
| From Sep 10, 2026 | Celebrity deepfakes with CNN branding spread against the midterms; actors told the press the words were not theirs | Verified record | B2 | AFP via CEDMO |
| From Sep 10, 2026 | Researchers tie the videos to the Matryoshka network (Operation Overload); the Antibot4navalny collective made the first attribution | Third-party attribution | C3 | CEDMO |
| Sep 18, 2026 | Classified US assessments, reported by the New York Times, say the Kremlin authorized a campaign to inject chaos into the midterms; officials called it less extensive than earlier cycles | Third-party attribution, anonymous sources | B3 | Political Wire |
| Sep 20 to 23, 2026 | Russian election officials claim 1,000, then 3,000, then 4,000 attack waves on the Duma vote from up to six countries, and admit a 30-to-60-minute remote-voting outage; nothing independent confirms the counts | Adversary claim | B4 | Vedomosti |

Table 10. Russia: Q3 evidence.

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

| Prediction | Most-likely line | Likelihood and grade | Competing alternative | Falsifier |
|---|---|---|---|---|
| RU-P1 Target set | Energy, telecom, transport, finance, defense supply base; Ukraine and NATO Europe primary | Likely, B2 | Concentration narrows to Ukraine-adjacent targets | Access moves off edge devices |
| RU-P2 Influence | Fake-branded content continues through the November 3 US midterms | Likely, B2 | Audience reach grows to mass scale (Unlikely) | A single item reaches a mass organic audience |
| RU-P3 Geography | NATO Europe and Ukraine-adjacent operations raise exposure | Likely, B2 | Targeting shifts to the US homeland | New-region telemetry before mid-horizon |
| RU-P4 Geopolitical | Collection and positioning dominate; disruption stays below the base case | Likely, B3 | Disruptive effect inside a Western lifeline sector | Access-to-effect transition |

Table 11. Russia: forecast and falsifiers.

| Condition (IF) | Selecting line | Example entity |
|---|---|---|
| Operates or supplies a NATO-Europe lifeline sector | GRU pre-positioning | An energy, transport, or telecom operator |
| Is a NATO-aligned government or logistics body | Hacktivist denial-of-service | A ministry, port, or logistics firm |
| Is a software vendor or managed-service provider | APT29 supply-chain access | A managed-service, cloud, or software provider |
| Is ransom-capable or uptime-sensitive | State-tolerated ransomware ecosystem | A manufacturer, healthcare provider, or service firm |

Table 12. Russia: the selection function.

### *North Korea: Operational*

The Reconnaissance General Bureau directs the cyber program, and the Lazarus Group and its TraderTraitor subset run the cryptocurrency thefts. Q3 advisories add the 313 General Bureau as a second organization behind WaterPlum and some IT workers. Three lines run together: cryptocurrency theft, fraudulent IT-worker placement, and espionage. Deception reads Operational for North Korea.

The state conceals more than it fabricates, so documented thefts carry full grade and denials carry a discount.

| Date | Development | Label | Grade | Source |
|---|---|---|---|---|
| Sep 18, 2026 | Seven-agency advisory led by Japan: WaterPlum (Contagious Interview) infects 30,000+ devices in 100+ countries, steals data from 7,000+ wallets, moves at least 1.7 billion yen; assessed to operate under the 313 General Bureau (some IT workers too) | Verified record | A1 | NPA |
| Sep 18, 2026 | Advisory describes interviewees using AI face-swapping software on video calls and cutting the video after minutes | Verified record | A1 | NPA |
| Sep 18, 2026 | Japanese police dismantle the country's first domestic laptop farm; workers moved assets worth several hundred million yen abroad | Verified record | A1 | NPA |
| Sep 24 to Oct 1, 2026 | Bitget loses about $387 million; Chainalysis attributes the theft to North Korea-linked actors and puts 2026 North Korean theft above $1 billion; no FBI statement by October 4 | Third-party attribution | B3 | Decrypt |

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

Table 13. North Korea: Q3 evidence.

| Prediction | Most-likely line | Likelihood and grade | Competing alternative | Falsifier |
|---|---|---|---|---|
| KP-P1 Target set | Exchanges, custodians, bridges, DeFi; remote-hire employers; defense suppliers | Likely, B2 | Pivot from theft to destruction | Destructive effect lands on a financial target |
| KP-P2 Verticals | Cryptocurrency and fintech first; software and IT hiring second | Likely, B2 | Concentration narrows to cryptocurrency alone | New sector named by a government |
| KP-P3 Geography | US remote-hire exposure and global crypto exposure run in parallel | Likely, B2 | Exposure shifts toward Japan and Europe | No new-region telemetry by mid-horizon |
| KP-P4 Attribution | FBI or another government names North Korea for the Bitget theft before January 15, 2027 | Roughly even chance | Third-party attribution stands alone | No official statement by January 15, 2027 |

Table 14. North Korea: forecast and falsifiers.

| Condition (IF) | Selecting line | Example entity |
|---|---|---|
| Holds, custodies, or moves cryptocurrency | Lazarus and subgroup theft at state scale | An exchange, custodian, DeFi protocol, or bridge |
| Hires remote technical staff | Fraudulent IT-worker placement and insider data theft | Any firm with remote software or IT hiring |
| Is a financial-technology or blockchain firm | Executive-targeted social engineering | A fintech, wallet, or blockchain provider |
| Is a defense or aerospace contractor | Espionage against weapons-relevant technology | A defense-industrial-base supplier |

Table 15. North Korea: the selection function.

### *Iran: Operational*

The IRGC Intelligence Organization and the IRGC Cyber-Electronic Command run one track. MOIS runs the other. Attributed clusters include APT35, APT42, APT34, MuddyWater, and CyberAv3ngers. Iranian tempo tracks the kinetic cycle, and the cycle turned on July 8, when the ceasefire collapsed.

Q3 supplies three supports for the one-point gain and one record that weighs against two of its sub-index points. A mixed record follows.

| Date | Development | Label | Grade | Source |
|---|---|---|---|---|
| Jul 8, 2026 | The US-Iran ceasefire collapses after Iranian attacks on ships off Oman; CENTCOM strikes more than 80 targets; the IRGC hits US bases in Kuwait and Bahrain | Verified record | B2 | Al Jazeera |
| Jul 22, 2026 | CISA updates AA26-097A: Iranian-affiliated actors exploit internet-exposed controllers across US infrastructure; similar activity tied to CyberAv3ngers (IRGC Cyber-Electronic Command) | Verified record | A2 | CISA |

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

| Date | Development | Label | Grade | Source |
|---|---|---|---|---|
| Jul 26 to 27, 2026 | More than 30 Minnesota water systems lose operational technology. No agency has named the attacker. Tenable assesses CyberAv3ngers; the Washington Post reports US intelligence suspects Iran; the President disputes an Iranian role | Third-party attribution | B3 | Help Net Security |
| About Jul 29, 2026 | Handala Hack claims the Minnesota attack; IRGC-aligned Mashregh News relays the claim | Adversary claim | E4 | Mashregh News |
| Aug 10, 2026 | Supreme Leader orders completion of a merger of the General Staff and Khatam al-Anbiya headquarters; names a General Staff chief; a former Khatam al-Anbiya cyber commander becomes IRGC deputy commander-in-chief; Foreign Policy reports the mandate names cognitive and hybrid threats | Verified record (decrees), third-party reading | B2 | Critical Threats |
| Aug 10, 2026 | Decree text, read in Persian: the new General Staff chief must answer conventional, new military, cognitive, and hybrid threats and complete the merger with Khatam al-Anbiya headquarters; a second decree tells the IRGC commander to prepare for powerful offensive operations | Verified record | A2 | Tabnak |
| Aug 27, 2026 | IRGC Intelligence Organization statement lists seven cognitive-war lines it expects, including erosion of the value of Hormuz and incitement of street unrest; its attributions to US, Israeli, and British services are adversary claims | Verified record (doctrine) | A2 | Nournews |
| Sep 10, 2026 | Anthropic reports Iranian state-aligned propaganda offices used its model as the working layer of influence operations; activity disrupted between December 2025 and August 2026 | Third-party attribution | B2 | Anthropic |
| Sep 15, 2026 | NCSC, FBI, and AIVD publish a joint advisory on CHOSEN BRICK spyware used by Iranian state cyber actors against dissidents, activists, and journalists since at least 2025; personal details of some victims appeared on pro-Iranian leak sites. The advisory names no ministry | Verified record | A2 | Joint advisory |
| Sep 15, 2026 | FBI flash report on the same malware (FBI name HEAVYGRAM) assesses that MOIS cyber actors likely use it and dates use to the fall of 2023; it updates the FBI's March 20, 2026 report | Verified record | A2 | FBI flash |
| Oct 1, 2026 | President Trump rejects an Iranian seven-day proposal; reports say bombing is expected to resume in November | Verified record (statement), third-party reading | B2 | CNBC |

Table 16. Iran: Q3 evidence.

**What supports the gain.** The AI Tradecraft Adoption move, 76 to 78, stands on the Anthropic disclosure, which shows state offices using AI as the working layer of influence operations. Doctrinal Maturity moved from 70 to 71 on the August 10 decrees, because the mandate names cognitive and hybrid threats. Operational Tempo moved from 76 to 77 on the AA26-097A update, with a limit: no agency has named the Minnesota attacker. Read in Persian, the decree text goes further than the press summaries: it tells the new General Staff chief to answer conventional, new military, cognitive, and hybrid threats, and a second decree tells the IRGC commander to prepare for powerful offensive operations.

**What weighs against it.** Exposure cuts against two Iranian gains. Three governments published indicators of compromise and detection advice for CHOSEN BRICK, and the FBI named MOIS. That record argues against credit for Adaptation (68 to 69) and OPSEC Sophistication (78 to 79). Treadstone 71 kept the two points in the edition and flags them for review on January 15, 2027.

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

Reversing the pair pulls the mean to 76.375 and the composite to 76. Either one alone leaves the mean at 76.5, which rounds to 77.

**What the edition does not claim.** The edition does not say a US agency attributed the Minnesota attack to Iran. Nor does it say three governments named MOIS, because only the FBI did. Iranian state-media text stands as evidence of doctrine and command, and no Iranian article stands as evidence of an operation here. State-aligned outlets relay hacktivist claims, and the edition carries those as adversary claims at E4.

| Prediction | Most-likely line | Likelihood and grade | Competing alternative | Falsifier |
|---|---|---|---|---|
| IR-P1 Target set | Exposed industrial-control operators; dissident-data holders; government and policy bodies; conflict-exposed firms | Likely, B2 | Collection narrows to surveillance only between spikes | Access moves off exposed controllers |
| IR-P2 Verticals | Water, energy, fuel; telecom and data holders; government; media and human rights | Likely, B2 | Concentration narrows to operational technology alone | A new sector is named |
| IR-P3 Geography | US, Israeli, and Gulf-host operations raise exposure during conflict windows | Likely, B2 | Exposure broadens to Europe | No new-region telemetry by mid-horizon |
| IR-P4 Command | The General Staff and Khatam al-Anbiya merger remains unfinished on January 15, 2027 | Likely, B3 | Merger completes early | Official announcement of completion |
| IR-P5 Kinetic cycle | Renewed large-scale US strikes on Iran by January 15, 2027 | Likely, B3 | Talks resume and the stalemate holds | No US strike wave by January 15, 2027 |

Table 17. Iran: forecast and falsifiers.

| Condition (IF) | Selecting line | Example entity |
|---|---|---|
| Operates internet-exposed industrial-control systems | CyberAv3ngers operational-technology disruption | A water, wastewater, energy, or fuel-systems operator |
| Holds population-scale personal data | MOIS and IRGC surveillance collection | An internet provider, telecom, or medical-records holder |
| Is a government, policy, media, or human-rights body | APT35 and APT42 espionage and surveillance | A policy institute, news outlet, or rights organization |
| Operates in or hosts US or Israeli facilities in the Gulf | Conflict-reactive targeting during kinetic windows | A firm with Gulf operations or base support |

Table 18. Iran: the selection function.

## Tearline 3: Tactical, for Analysts, Hunters, and Collection Managers

For each adversary, start at the attribution and tradecraft, confirm the evidence anchoring and the grades, and split verified fact from adversary claim before acting. Convert each watch item into a hunt or detection task against the named cluster. Read the edition for attribution, grading, and falsifier-driven priorities. Rows marked Carried come from the July 15 edition and were not re-verified in the Q3 pass, and rows marked Q3 are new.

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

### *China*

| Anchor | Source basis | Grade | Edition |
|---|---|---|---|
| Volt Typhoon pre-positioning across communications, energy, transport, water | CISA, NSA, FBI joint advisory with Five Eyes | A2 | Carried |
| Salt Typhoon backbone espionage across 80-plus countries | Joint advisory across 13 governments | B2 | Carried |
| MSS contractor practices | i-SOON contractor leak, February 2024 | B2 | Carried |
| Spamouflage altered event flyers | Graphika | B2 | Q3 |
| Uyghur tracking and recruitment by an AI-assisted PRC-aligned actor | Anthropic | B2 | Q3 |

Table 19. China: attribution anchors.

Hunt priorities: edge-device initial access, living-off-the-land persistence in edge and identity environments, carrier and backbone exposure, cloud and identity abuse, and the access-to-effect transition as the earliest warning of the one observable. Beijing's denials and counter-accusations read as adversary-originated and route to the deception axis.

### *Russia*

| Anchor | Source basis | Grade | Edition |
|---|---|---|---|
| APT28 intrusion set tied to GRU Unit 26165 | France ANSSI attribution, April 2025 | A | Carried |
| Doppelganger influence infrastructure sanctioned | European Union sanctions on the Social Design Agency | A2 | Carried |
| GRU edge-device targeting of Western lifeline infrastructure | Amazon and Microsoft reporting | B2 | Carried |
| LAUNDRY BEAR exploitation of Zimbra CVE-2025-66376 | CISA advisory AA26-204A | A2 | Q3 |
| AI-agent intrusion cluster GTG-20006 | Anthropic | B2 | Q3 |

Table 20. Russia: attribution anchors.

Hunt priorities: internet-facing appliance review against APT28 and APT44, webmail server patching and two-factor token review against LAUNDRY BEAR, token and OAuth abuse against APT29, and provenance and coordinated-inauthentic-behavior signals on suspected synthetic media. The influence content claims route to the deception axis.

### *North Korea*

| Anchor | Source basis | Grade | Edition |
|---|---|---|---|
| Bybit theft of about $1.46 billion in 2025, largest on record | FBI | A2 | Carried |
| IT-worker scheme inside 100-plus firms | US Department of Justice | A2 | Carried |
| $577 million in two April 2026 attacks; 76 percent of 2026 crypto-hack losses through April | Blockchain-intelligence telemetry | B2 | Carried |

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

| Anchor | Source basis | Grade | Edition |
|---|---|---|---|
| WaterPlum campaign: 30,000+ devices, 7,000+ wallets, 313 General Bureau | Japan National Police Agency and six partners | A1 | Q3 |
| Bitget theft attributed to North Korea-linked actors | Chainalysis via Decrypt | B3 | Q3 |

Table 21. North Korea: attribution anchors.

Hunt priorities: custody and cryptographic-material controls, bridge and multisig governance, remote-hire identity and laptop-farm screening, handling of unsolicited recruiter outreach, and the move from theft to destructive effect as the warning of the one observable.

### *Iran*

| Anchor | Source basis | Grade | Edition |
|---|---|---|---|
| CyberAv3ngers operations against exposed industrial-control systems | Joint government advisory; Treasury designation of six IRGC-CEC officials | A2 | Carried |
| APT42 surveillance against dissidents and policy targets | Vendor reporting | B2 | Carried |
| AA26-097A update on Iranian-affiliated controller exploitation | CISA and partners | A2 | Q3 |
| CHOSEN BRICK (FBI name HEAVYGRAM) spyware against dissidents | NCSC, FBI, AIVD joint advisory; FBI flash | A2 | Q3 |
| State propaganda offices using AI in influence operations | Anthropic | B2 | Q3 |

Table 22. Iran: attribution anchors.

Hunt priorities: internet-exposed industrial-control inventory and segmentation, review of reusable code modules in controller projects, phishing and identity hardening against APT35 and MuddyWater, dissident-data protection against APT42, and false-claim verification during conflict windows. Iran runs false attack claims, hacktivist fronts over state direction, and persona churn, so adversary-originated claims are discounted and carried apart.

## Tearline 4: Technical, for Detection Engineers and the Security Operations Center

Technical readers work from machine artifacts and forensic residue. The index publishes no indicators, hashes, network addresses, or detection content. Pull those from the threat-intelligence feed, and expect them to expire in hours or days. The public edition names only the tooling that Q3 government advisories name.

- **China.** The Q3 evidence window carries no new government advisory on Chinese tooling. Edge-device exploitation and pre-positioning stay as the read carried from earlier editions, and the Q3 pass did not re-verify them.
- **Russia.** CISA advisory AA26-204A names LAUNDRY BEAR (Void Blizzard) exploitation of a Zimbra flaw, CVE-2025-66376, active since at least July 2025. Grade A2.
- **North Korea.** The NPA advisory names five malware families (BeaverTail, InvisibleFerret, OtterCookie, OtterCandy, and StoatWaffle), a Visual Studio Code tasks file that runs when a trusted folder opens, and AI face-swap software on video interviews. Grade A1. All five families were public before the advisory.

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

- **Iran.** CISA advisory AA26-097A, updated July 22, covers Iranian-affiliated exploitation of internet-exposed controllers. The NCSC, FBI, and AIVD advisory names CHOSEN BRICK spyware, and the FBI flash calls it HEAVYGRAM. Grade A2. No document equates Handala's claimed "Na'em" tool with CHOSEN BRICK.

Convert each named item into a detection requirement for the feed to answer. The Technical tearline stops at names and grades.

***Read-Back Risk***

Publication names the edge-device vector, the laundering and IT-worker patterns, the influence networks, and the exposed-control-system exposure. The adversary reads the same lines. Each named pattern already sits in public vendor and government reporting, so the forecast adds no exposure beyond the public record. Target-specific access detail stays out of the public edition.

## The 42-Actor Field at Catalog Level

The Big Four lead a catalog of 42 named adversaries across ten operational clusters, with seven Iranian-axis component annexes held in the paid editions. Below the four state powers, 38 actors hold tiered positions. No actor below the Big Four reaches the peer-state band. None reaches Tier 0. Catalog scores for the 38 carry forward from the July 15 release. The Q3 refresh re-scored Iran only.

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

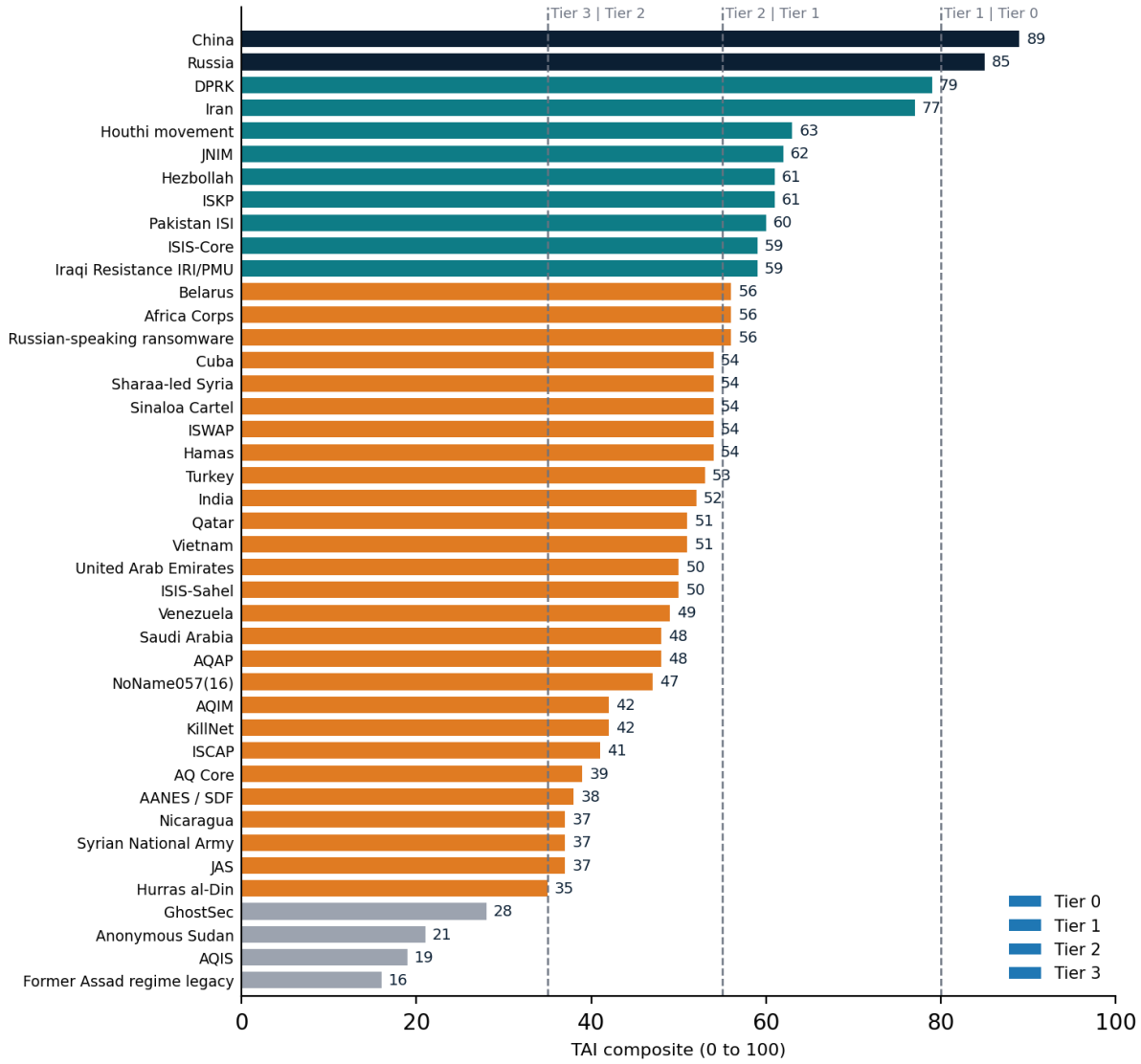



Figure 14. The 42-actor field, ranked and colored by tier band. Dashed lines mark the Tier 3 to Tier 2 (35), Tier 2 to Tier 1 (55), and Tier 1 to Tier 0 (80) boundaries.

| # | Cluster | Actor | Composite | Tier |
|---|---|---|---|---|
| 1 | Big Four | China | 89 | Tier 0 |
| 2 | Big Four | Russia | 85 | Tier 0 |
| 3 | Big Four | DPRK | 79 | Tier 1 |
| 4 | Big Four | Iran | 77 | Tier 1 |
| 5 | Cluster 2 | Houthi movement | 63 | Tier 1 |
| 6 | Cluster 7 | JNIM | 62 | Tier 1 |
| 7 | Cluster 2 | Hezbollah | 61 | Tier 1 |
| 8 | Cluster 7 | ISKP | 61 | Tier 1 |
| 9 | Cluster 5 | Pakistan ISI | 60 | Tier 1 |
| 10 | Cluster 7 | ISIS-Core | 59 | Tier 1 |

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

| # | Cluster | Actor | Composite | Tier |
|---|---|---|---|---|
| 11 | Cluster 2 | Iraqi Resistance IRI/PMU | 59 | Tier 1 |
| 12 | Cluster 1 | Belarus | 56 | Tier 2 |
| 13 | Cluster 1 | Africa Corps | 56 | Tier 2 |
| 14 | Cluster 9 | Russian-speaking ransomware | 56 | Tier 2 |
| 15 | Cluster 3 | Cuba | 54 | Tier 2 |
| 16 | Cluster 4 | Sharaa-led Syria | 54 | Tier 2 |
| 17 | Cluster 8 | Sinaloa Cartel | 54 | Tier 2 |
| 18 | Cluster 7 | ISWAP | 54 | Tier 2 |
| 19 | Cluster 2 | Hamas | 54 | Tier 2 |
| 20 | Cluster 6 | Türkiye | 53 | Tier 2 |
| 21 | Cluster 6 | India | 52 | Tier 2 |
| 22 | Cluster 6 | Qatar | 51 | Tier 2 |
| 23 | Cluster 6 | Vietnam | 51 | Tier 2 |
| 24 | Cluster 6 | United Arab Emirates | 50 | Tier 2 |
| 25 | Cluster 7 | ISIS-Sahel | 50 | Tier 2 |
| 26 | Cluster 3 | Venezuela | 49 | Tier 2 |
| 27 | Cluster 6 | Saudi Arabia | 48 | Tier 2 |
| 28 | Cluster 7 | AQAP | 48 | Tier 2 |
| 29 | Cluster 10 | NoName057(16) | 47 | Tier 2 |
| 30 | Cluster 7 | AQIM | 42 | Tier 2 |
| 31 | Cluster 10 | KillNet | 42 | Tier 2 |
| 32 | Cluster 7 | ISCAP | 41 | Tier 2 |
| 33 | Cluster 7 | AQ Core | 39 | Tier 2 |
| 34 | Cluster 4 | AANES / SDF | 38 | Tier 2 |
| 35 | Cluster 3 | Nicaragua | 37 | Tier 2 |
| 36 | Cluster 4 | Syrian National Army | 37 | Tier 2 |
| 37 | Cluster 7 | JAS | 37 | Tier 2 |
| 38 | Cluster 7 | Hurras al-Din | 35 | Tier 2 |
| 39 | Cluster 10 | GhostSec | 28 | Tier 3 |
| 40 | Cluster 10 | Anonymous Sudan | 21 | Tier 3 |
| 41 | Cluster 7 | AQIS | 19 | Tier 3 |
| 42 | Cluster 4 | Former Assad regime legacy | 16 | Tier 3 |

Table 23. The ranked catalog at catalog level. Belarus, Africa Corps, and the Russian-speaking ransomware ecosystem score 56 and read Tier 2, because the published band draws the Tier 1 line in the gap above them.

The ten clusters group the catalog by operational character: Belarus and Wagner-successor structures, the Iranian Axis, the ALBA bloc, post-Assad Syrian factions, Asian authoritarian states, gray-zone state cyber actors, Salafi-jihadist networks, cartels and paramilitaries, cybercrime ecosystems, and hacktivist networks. Salafi-jihadist networks form the largest cluster at 12 actors.

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

## The ASA Evidence Standard

Every judgment in the edition rests on evidence, and the ASA Evidence Standard grades how good that evidence is. The Admiralty letter and digit remain the starting read. The full screen follows. Another 28 factors, grouped into nine clusters, produce three scores: the T-Score rates evidence quality, the D-Score rates how much deception the picture carries, and the F-Score rates forecast confidence. Public Edition 1.2 weights the quality clusters equally.

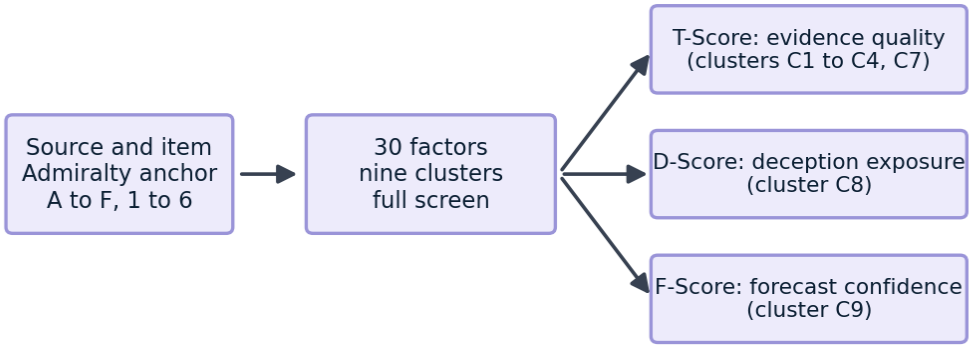



Figure 15. From Admiralty anchor to tri-score.

| Score | Built from | Rule |
|---|---|---|
| T-Score | Mean of the applicable quality clusters C1, C2, C3, C4, and C7 | Capped at 100 minus the higher of the two risk clusters, C5 and C6 |
| D-Score | Mean of the examined C8 factors, floor of 25 | Needs three of five factors; fewer print the floor with a note |
| F-Score | Mean of the usable C9 factors | A factor from an item with T under 40 is excluded; three usable factors needed |

Table 24. The tri-score in Public Edition 1.2.

| T band | Likelihood cap on any forward judgment |
|---|---|
| Strong (80 and above) | Any band |
| Adequate (60 to 79) | Likely |
| Weak (40 to 59) | Roughly even chance |
| Insufficient (under 40) | No forward judgment from the item |

Table 25. T bands and likelihood caps.

A D-Score of 55 or more drops the cap one band. A second reader is required when D is 55 or more, or when any score sits within five points of a band edge.

Four built-in rules protect the grades. A self-serving claim cannot grade above C on reliability. An admission against interest is exempt from that rule. A single uncorroborated source holds the Information Validity cluster (C2) at 80. Factors one and eight take their scores from the Admiralty letter and digit. The edition prints Admiralty grades on every anchor, and the standard itself

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

appears as the ASA Evidence Standard Public Edition 1.2, concept DOI 10.5281/zenodo.23137881.

## What the Paid Editions Add

| Edition | Price | What the subscriber receives |
|---|---|---|
| Tier 0 Public | Free | The Big Four at full tearline depth, the 42-actor field at catalog level, the scoring framework, and a board-level insight layer |
| Tier 1 Analyst | $25,000 a year | Everything in Tier 0, plus the seven actors below the Big Four at full eight-sub-index depth (11 scored in all) and the analyst operating layer: collection and hunt priorities, an indicator-of-change tripwire register, quarter-over-quarter movers, and a responsibility matrix |
| Tier 2 Institutional | $75,000 a year | Everything in Tier 1, plus 38 actors at STEMPLES Plus depth and control mapping to NIST and CIS |
| Tier 3 Executive Desk | $250,000 a year | Everything in Tier 2, plus the complete field, a composite weighted to the subscriber's organization, and quarterly board briefings from a named senior analyst |

Table 26. The four editions.

Layers are cumulative. The drill-down chain is the method behind the product: composite to sub-index to STEMPLES Plus input to indicator evidence to the source document. A composite without drill-down is an assertion. With drill-down it becomes a defensible analytic product.

## Limits of the Q3 Record

- The search of Justice Department, Treasury, and doctrine records for China and North Korea did not finish, so the edition treats the absence of a Chinese government advisory in the window as a gap.
- Microsoft's CaptiveCrunch report on Midnight Blizzard reached the review only by reference through Anthropic. The edition does not rely on it.
- Anthropic names Iranian institutions in its report. The institution names in the Iran chapter come from press accounts of the report and need a read against the report text.
- Rows marked Carried come from the July 15 edition and were not re-verified in the Q3 pass.
- Five source sites block scripted checks. They open in a normal browser.
- Admiralty grades are analyst judgments.
- The edition carries no dollar figure, no indicator feed, and no peer ranking, by design.

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

## Appendix A: Acronyms and Terms

| Term | Meaning |
|---|---|
| AEI | Adaptation/Evolution Index, a TAI sub-index |
| AIVD | Netherlands General Intelligence and Security Service |
| ASA | Adversary Scoring Architecture; the ASA Evidence Standard grades evidence in 30 factors across nine clusters |
| ATA | AI Tradecraft Adoption, a TAI sub-index |
| Admiralty grade | Letter for source reliability (A to F) and digit for information credibility (1 to 6) |
| Boundary review zone | Composites from 75 to 85, where a standing senior-analyst review applies |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CWV | Cognitive Warfare Velocity, a TAI sub-index |
| DM | Doctrinal Maturity, a TAI sub-index |
| DPRK | Democratic People's Republic of Korea (North Korea) |
| FBI | Federal Bureau of Investigation |
| GRU, FSB, SVR | Russian military intelligence, domestic security service, and foreign intelligence service |
| IRGC | Islamic Revolutionary Guard Corps |
| MOIS | Iranian Ministry of Intelligence and Security |
| MSS | Chinese Ministry of State Security |
| NCSC | United Kingdom (UK) National Cyber Security Centre |
| NPA | Japan National Police Agency |
| NV | Narrative Volume, a TAI sub-index |
| OPS | OPSEC Sophistication, a TAI sub-index |
| OT | Operational Tempo, a TAI sub-index |
| PLA | People's Liberation Army |
| STC | Sectoral Targeting Concentration, a TAI sub-index |
| STEMPLES Plus | The Treadstone 71 domain framework behind the sub-index roll-ups |
| TAI | The Treadstone 71 Adversary Index |
| Tearline | A reader layer cut by audience, not by classification |

Table 27. Acronyms and terms.

## Appendix B: Sources

| # | Publisher | Date | Grade |
|---|---|---|---|
| 1 | NCSC / FBI / AIVD joint advisory (UK-format PDF, hosted by IC3) | Sep 15, 2026 | A2 |
| 2 | FBI FLASH (HEAVYGRAM), update to FLASH-20260320-001 | Sep 15, 2026 | A2 |
| 3 | FBI FLASH-20260320-001 | Mar 20, 2026 | A2 |
| 4 | CISA et al., AA26-097A (updated Jul 22, 2026) | Apr 7, 2026; Jul 22, 2026 | A2 |
| 5 | IC3 copy of AA26-097A update | Jul 22, 2026 | A2 |
| 6 | Critical Threats Project | Aug 10, 2026 | B2 |

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

| # | Publisher | Date | Grade |
|---|---|---|---|
| 7 | Iran International | Aug 10, 2026 | C2 |
| 8 | Foreign Policy | Aug 13, 2026 | B3 |
| 9 | Al Jazeera | Jul 3, 2026 | B2 |
| 10 | NPR | Jul 4, 2026 | B2 |
| 11 | CNN | Jul 6, 2026 | B2 |
| 12 | Time | Jul 5, 2026 | B2 |
| 13 | Al Jazeera | Mar 8, 2026 | B2 |
| 14 | Help Net Security | Jul 30, 2026 | B2 |
| 15 | Washington Post | Jul 30, 2026 | B3 |
| 16 | Tenable | Jul 28, 2026 | B3 |
| 17 | The Register | Jul 29, 2026 | B3 |
| 18 | ABC News | Jul 31, 2026 | B2 |
| 19 | NBC News | Jul 2026 | B2 |
| 20 | Al Jazeera | Jul 30, 2026 | B2 |
| 21 | Mashregh News (IRGC-aligned) | About Jul 29, 2026 | E4 |
| 22 | Tabnak, citing Fars | Early Aug 2026 | E5 |
| 23 | CISA, NSA, FBI and partners, AA26-204A | Jul 23, 2026 | A2 |
| 24 | Microsoft Threat Intelligence | Jul 31, 2026 | B3 |
| 25 | CEDMO (AFP text) | Sep 2026 | B2 |
| 26 | MS NOW | Sep 2026 | B3 |
| 27 | Mother Jones | Sep 2026 | C3 |
| 28 | Political Wire (New York Times report) | Sep 18, 2026 | B3 |
| 29 | Election Law Blog | Sep 2026 | C3 |
| 30 | Anthropic | Sep 10, 2026 | B2 |
| 31 | Anthropic (PDF) | Sep 10, 2026 | B2 |
| 32 | Al Jazeera | Sep 11, 2026 | B2 |
| 33 | U.S. News (Reuters) | Sep 10, 2026 | B2 |
| 34 | Technology.org | Sep 14, 2026 | C3 |
| 35 | Graphika | Jul 13, 2026 | B2 |
| 36 | The Epoch Times | Aug 30, 2026 | D3 |
| 37 | Japan National Police Agency (English PDF) | Sep 18, 2026 | A1 |
| 38 | Japan National Police Agency (Japanese page) | Sep 18, 2026 | A1 |
| 39 | SecurityWeek | Sep 2026 | B2 |
| 40 | Forbes | Sep 19, 2026 | B2 |
| 41 | Decrypt | Oct 1, 2026 | B3 |
| 42 | Brave New Coin | Sep 2026 | B3 |
| 43 | CryptoRank | Oct 1, 2026 | C3 |
| 44 | JFeed | May 2026 | C3 |

Table 28. The 44 sources behind the Q3 record. Grades show reliability and credibility separately and never average.

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

Copyright 2026 Treadstone 71 LLC. All rights reserved. 

## Copyright, Trademarks, and Production

**Copyright.** Copyright 2026 Treadstone 71 LLC. All rights reserved. Read this edition, share it in full and unaltered, and cite it. Other uses, including excerpts of scores, charts, or text, need written permission from Treadstone 71 LLC.

**Trademarks.** The ASA Evidence Standard, STEMPLES Plus, The Adversary Index, TAI, and Advanced Analytic Dominance are trademarks of Treadstone 71 LLC.

**Production disclosure.** The analyst directed the forecast. An AI agent assisted drafting, figure production, and consistency checks. The analyst approves each judgment and grade before release. The edition follows the Sherman Kent probability spectrum, the ASA Evidence Standard tri-score with Admiralty grading, base-rate anchoring, structured alternatives with falsifiers, and the verification record.

**Contact.** Treadstone 71 LLC, Half Moon Bay, California. treadstone71.com. Press and research requests use the contact form on the site.

Copyright 2026 Treadstone 71 LLC