The Treadstone 71 Adversary Index

Tier 0 Free Edition · Q2 2026 · Big Four in depth across three tearlines, full 42-actor field

Treadstone 71 Adversary Index · Big Four in depth, full 42-actor field

Issue date: July 15, 2026 · Horizon through October 13, 2026

China 89 · Russia 85 · DPRK 79 · Iran 78

Tier 0 Free Edition · v1.0 · the free public report · scored to the v2.1 catalog · methodology v3.0 · full 42-actor catalog releases across the paid tiers on July 15, 2026

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 78 sit a step below, inside Tier 1. China alone stands clear of a tier line; Russia, North Korea, and Iran sit inside the 75–85 boundary review zone and carry a standing senior-analyst review. The scores hold the quarter (Likely). Each adversary runs reinforcing operations against a different center of gravity — China against the United States 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: the score holds until quiet activity turns into a real effect, and current evidence shows no such turn for any of the four.

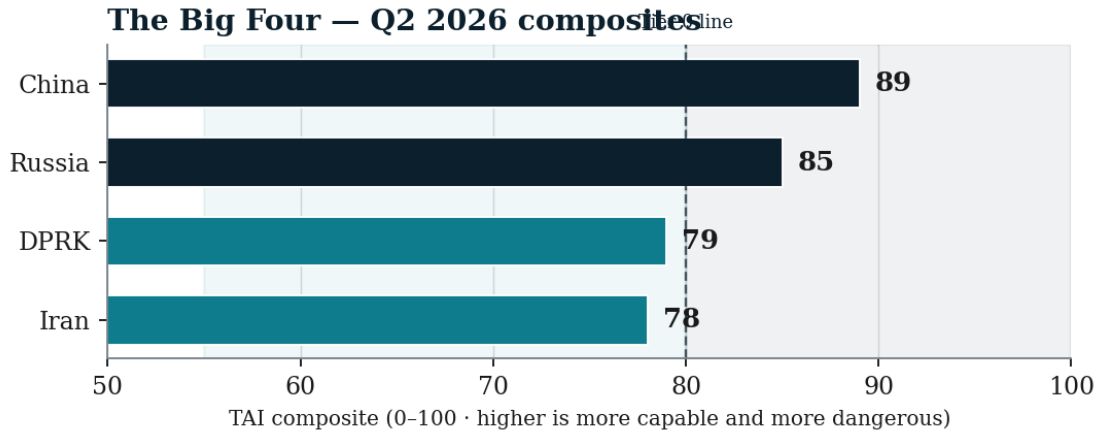


Figure A1. The Big Four composites with the tier-band backdrop and the Tier 0 line. China alone clears a tier boundary; Russia, the DPRK, and Iran sit inside the 75 to 85 review zone.

China ranks first at 89, Russia second at 85, North Korea third at 79, and Iran fourth at 78, the spread held flat from the Q1 2026 catalog through the October 13 resolution. China and Russia run the broadest sector coverage, so a lifeline operator or a technology firm often sits on more than one targeting line at once. A firm gets pulled in through its sector, its region, or a single dependency — a carrier link, a remote-hire pipeline, an exposed control system — not through

any quarrel of its own with a capital. The China-nexus loss is collection; the North Korean loss is theft; the Russian and Iranian lines add disruption against lifeline and operational-technology targets. Each adversary carries one observable that changes its read; until one fires, the four scores hold.

Movers, quarter over quarter. Iran moved plus 2, from 76 to 78, on the espionage-to-destruction crossing: a destructive wiper deployment in March 2026 and IRGC-linked activity against United States water and energy systems. The other three Big Four composites held flat from the Q1 2026 cut — China 89, Russia 85, North Korea 79. The movement sat in the field below them. The June 2026 Cluster 2 reconciliation lifted the Houthi movement from 57 to 63, the largest single move, and the Houthi now lead the field below the Big Four. Hamas fell from a paired 60 to 54 and crossed from Tier 1 into Tier 2; Palestinian Islamic Jihad split out at 46 as a separate component annex. Hezbollah corrected from an unsupported 64 to 61, and the Iraqi Resistance front groups rose from 58 to 59. The band below the Big Four moved from eight Tier 1 actors to seven. No Big Four score crossed a tier line, so no posture change follows from the four; the field reorder is the quarter's signal. The Houthi and Hamas moves sit out of the five-point tolerance and carry a senior-analyst review hold under Rubric Sections 6.5 and 7.6; the values publish with that hold noted and refine on sign-off if the review moves them.

Read this first — three reads the ranking hides

A ranking tells the board the order. It does not tell the board where the field is going, or why an adversary selects the organization. Three reads carry this quarter for a board, and each states the finding and why it is not obvious from the number.

One. The AI line splits the field. The widest gap in the index is not between China and the floor; it is the AI tradecraft line that divides the four states from every non-state actor. AI capability compounds: an actor with technical depth pulls further ahead as tooling matures, and an actor without it plateaus. The ranking is a lagging indicator. The adversary that surprises the board in eighteen months is the one climbing the AI axis now, not the one ranked highest today.

Two. The quarter moved below the waterline. The four leaders held flat. Every point of movement this quarter sat in the field beneath them. The threat did not intensify at the top; it redistributed downward, into the band where actors are cheaper to run, harder to attribute, and more likely to reach an organization that is not a government. The stability of the top is the signal, not the reassurance.

Three. The board is selected by intersection, not by rank. No adversary targets the organization because it scores high. It targets the organization because its sector, its region, and one dependency land together on a targeting line. The ranking is context; the intersection is the exposure. A board that reads only the leaderboard watches the wrong number.

How to read the edition

The edition runs in three labeled tearlines, split by audience rather than by classification. The Strategic tearline speaks to the board and the C-suite. The Operational tearline speaks to risk, governance, security leadership, and the intelligence function. The Tactical-Technical tearline speaks to analysts, hunters, and detection engineers. The four composites hold identical across

all three tiers; each tier states them at the depth that reader needs. The flow runs continuous — a reader descends as far as the role asks and no farther. Within each tier the four adversaries appear in composite order: China, Russia, the Democratic People's Republic of Korea, and Iran.

A short legend carries the probability and evidence terms. Sherman Kent terms attach defined bands; Likely spans 55 to under 85 percent. Evidence grades follow the ASA Evidence Standard v0.3, the Treadstone 71 expansion of the NATO Admiralty Code into 30 factors across nine clusters. The classic Admiralty letter–number anchor — source reliability A–F, information credibility 1–6 — survives as two factors inside the 30, so a grade such as B2 reads usually reliable, probably true and then rides the full screen. The output is the tri-score: T for evidence quality, D for deception likelihood, F for forecast confidence. An indicator of change (IoC) names a numbered tripwire; when it fires, the model revises the named judgment. Appendix C carries the full standard; Appendix A defines every term.

What the index scopes in, and what it leaves to other layers

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 worth of the reader's crown jewels, and the maturity of the reader's controls. A figure printed without those inputs misleads, and a careful reader discounts it on sight. The index stays a standard, comparable product that reads the same for every consumer. The money question moves to a per-client layer that prices impact against that client's own environment — the work of the embedded officer engagement and the Certified and Distinguished bands. The missing dollar figure is a deliberate line between the published product and the client-specific layer, not an omission.

No league table against peers, on purpose. A common request is a ranking — show how we compare to firms like us. For the threats that make the Big Four dangerous, the comparison misleads. 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. Only opportunistic crime — commodity ransomware and mass scanning — drifts toward the softer target, and even there the criminal line selects on payment capacity and reachability more than on any ranking. A peer ranking invites false comfort: a firm reads itself as above average and stands down while the targeted threat comes anyway. The useful version of the question is threat prevalence — which adversaries target the reader's sector and region, and how often — and the index carries it in the sector-and-region matrix and the commercial selection function.

No indicator feed, on purpose. The index does not publish indicators of compromise, detection signatures, or a technique-by-technique mapping. Those layers sit in products the reader already buys: a threat-intelligence feed, an endpoint platform, a detection-content library. The index runs above them, on attribution, scoring, forecast, and decision. The Treadstone 71 method holds the common technique frameworks outside the unit of analysis on purpose, so the forecast reasons about adversary behavior and intent rather than re-cataloging tactics that vendors already map. A reader who needs indicators pulls them from the feed and

reads the index for what the feed does not give: the strategic picture, the confidence, and the move.

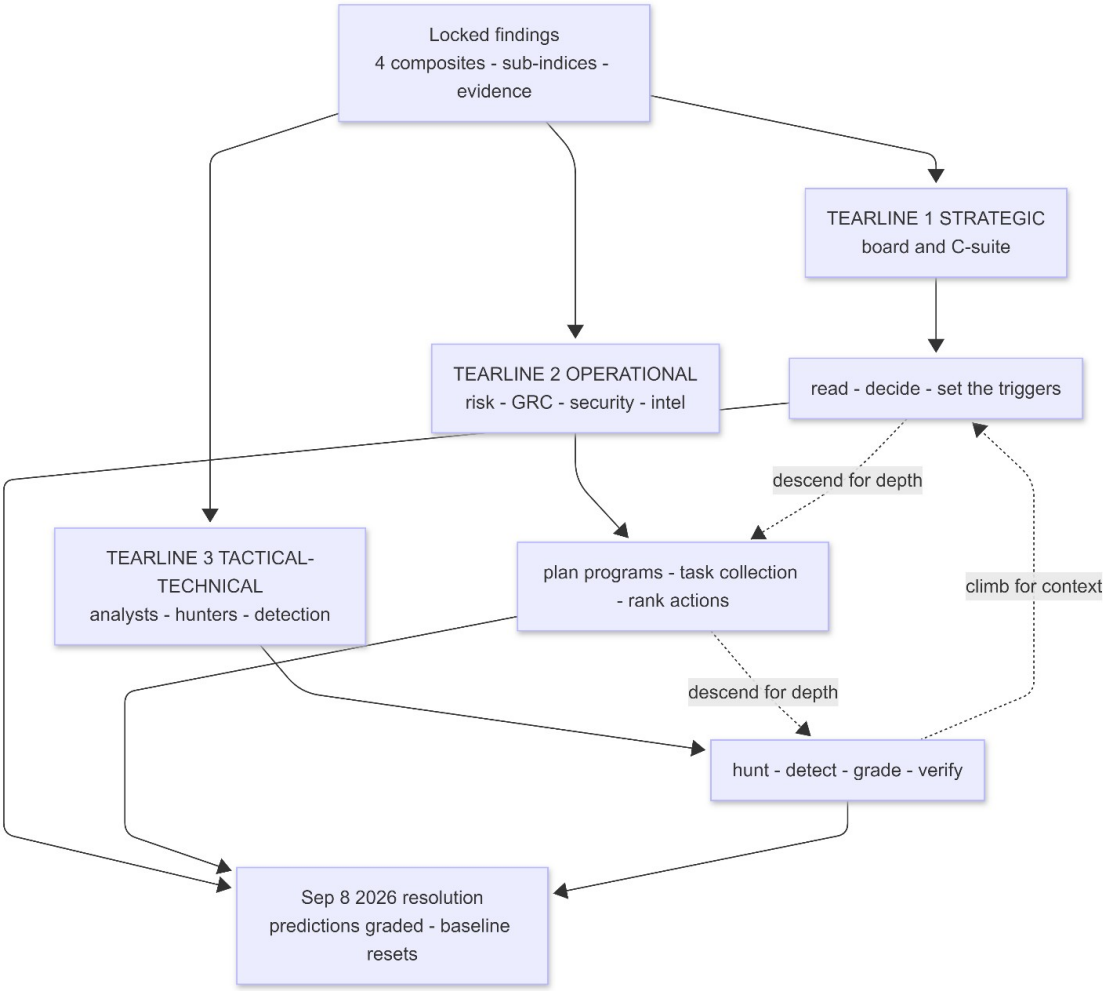
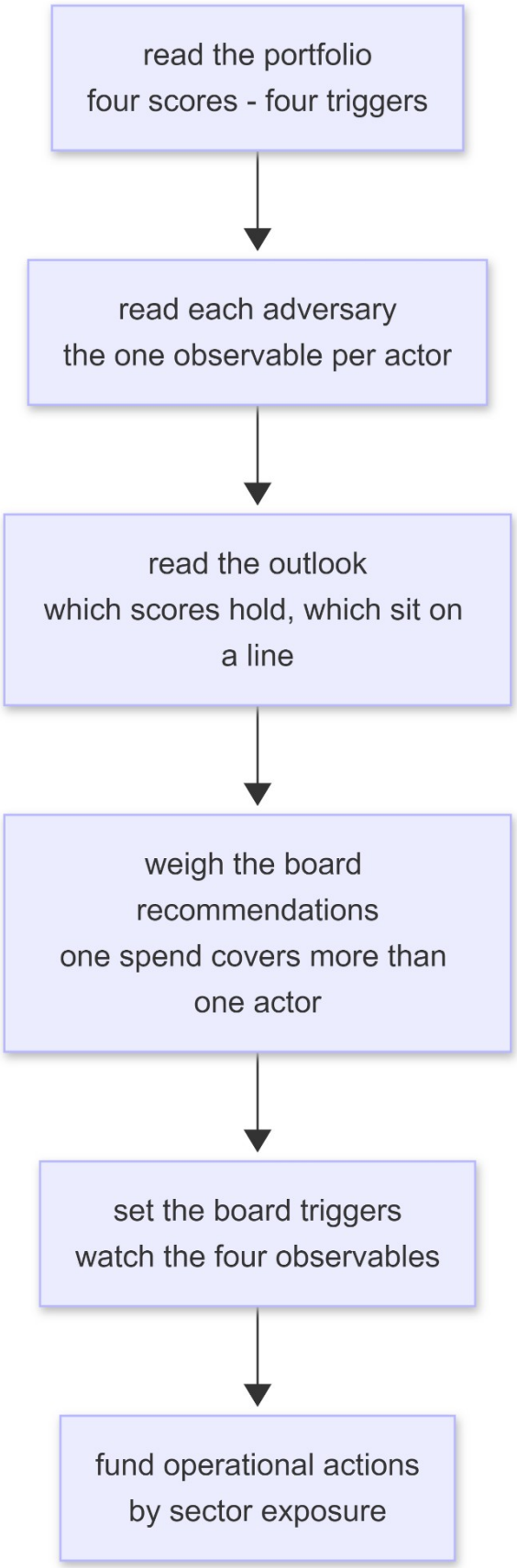


Figure A. Whole-report flow. Same findings, three reader paths, one resolution.

The field at a glance

Adversary	Composite	Tier	Reading
China	89	Tier 0	Catalog lead; outside the boundary review zone
Russia	85	Tier 0	Inside the 75–85 boundary review zone
North Korea (DPRK)	79	Tier 1 upper	Inside the boundary review zone; senior-analyst review at the tier line
Iran	78	Tier 1	Inside the boundary review zone; senior-analyst review at the tier line


read the portfolio
four scores - four triggers
read each adversary
the one observable per actor
read the outlook
which scores hold, which sit on a line
weigh the board recommendations
one spend covers more than one actor
set the board triggers
watch the four observables
fund operational actions
by sector exposure

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.

1. Know your sector and region. The index selects a firm 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. The field selection guide does the same for the 38 actors below the Big Four.

3. Fund the converged controls in order. Lead with edge-device and identity hardening — one spend answers Chinese, Russian, and Pakistani state intrusion that breaks in through the same equipment. Then insider and remote-hire screening, then operational-technology isolation, then restore-tested backups. The convergence-sizing table gives the risk cut per program.

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. The portfolio trigger board carries the four.

5. Resolve at October 13. Each prediction enters the record at issue and grades at the October 13 horizon. The verification record makes the check mechanical.

How to use the tearline. Read the portfolio paragraphs and the trigger board for the picture, then read each adversary's strategic read and the board recommendations table for the moves. The score runs 0 to 100; higher means more capable and more dangerous. The forecast issues July 1, 2026 and resolves at the October 13, 2026 horizon — a single quarterly window, anchored to the fixed resolution date. A score of 80 or above is the top tier (Tier 0), the peer-state threats; 55 to 79 is Tier 1; the lower bands step down from there[1]. Hand the rest of the edition to the security team. The flow below shows the path.

Figure B. Strategic reader path.

Four state adversaries lead the field. China holds 89 and Russia 85 in the top tier; the Democratic People's Republic of Korea at 79 and Iran at 78 sit a step below. China is the catalog lead. The scores hold the quarter. Each adversary runs reinforcing operations against a different center of gravity: China presses the United States and its Indo-Pacific allies, Russia

[1] The Treadstone 71 Adversary Index scores each adversary from 0 to 100; higher means more capable and more dangerous. Tier 0 (80–100) marks peer-state threats, Tier 1 (55–79) the next band, with Tier 2 (35–54) and Tier 3 (0–34) below. A score near a tier line, such as Russia at 85 or the DPRK at 79, sits under standing senior-analyst review.

presses NATO Europe and the firms inside Western lifeline sectors, North Korea drains the cryptocurrency sector to fund the regime, and Iran tracks the kinetic cycle in the Middle East.

A firm gets pulled in through its sector, its region, or a single dependency — a carrier link, a remote-hire pipeline, an exposed control system — not through any quarrel of its own with a capital. Among the four, China and Russia run the broadest sector coverage, so a lifeline operator or a technology firm often sits on more than one targeting line at once.

One pattern repeats across the four: the score holds until quiet activity turns into a real effect. China and Russia hold access rather than act; North Korea steals rather than destroys; Iran watches between conflicts. Each carries a single observable that changes its read. The board watches the four signals below; until one fires, the four scores hold.

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 United States lifeline sector, or a Taiwan exercise paired with cyber effect	Score holds; espionage and pre-positioning dominate	Read shifts from collection to coercion; Most Dangerous (Taiwan) elevates
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 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 78	Tier 1, boundary zone	A renewed Israel or United States kinetic exchange	Score holds; surveillance at tempo, the disruptive line low	The disruptive operational-technology line rises within days; activate OT-incident playbooks

The full field in one line

The Big Four lead a catalog of 42 named adversaries plus seven Iranian-Axis component annexes across nine operational clusters. Below the four, the Houthi movement leads the field

at 63 after the June 2026 reconciliation, down to the former Assad regime networks at 16; the split runs seven actors in Tier 1, 27 in Tier 2, and four in Tier 3, and no actor below the Big Four reaches the peer-state band. The full ranked catalog, the cluster-by-cluster selection guide, and the per-actor depth sit in the Operational tearline under "The full 42-actor field," and in the companion addendum, where the operator who needs them works them.

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 and the People's Liberation Army 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. The score holds at 89 through the October 13 resolution (Likely). One change moves the picture — access-holding turning into a disruptive effect in a United States lifeline sector, or a Taiwan exercise paired with a cyber effect — and current evidence shows no such turn.

Full BLUF. China ranks first in the field at 89, above Russia 85, North Korea 79, and Iran 78, and stays outside the 75–85 boundary review zone the other three sit inside. Energy, communications, transport, water, the technology and semiconductor base, logistics, and finance each sit on a China targeting line, the United States primary and Indo-Pacific allies elevated. Espionage, not extortion, carries the loss — the prize is the firm's intellectual property and its communications.

China runs the deepest state-aligned integration of cyber, cognitive, and AI tradecraft in the field. The Ministry of State Security and the People's Liberation Army hold quiet access inside United States communications, energy, transportation, and water systems on the Volt Typhoon pattern, ready for a Taiwan contingency rather than acting now. A telecommunications-backbone espionage campaign on the Salt Typhoon pattern reached the networks of at least nine major United States carriers and more than 80 countries, and the Federal Bureau of Investigation confirmed in February 2026 that the activity remains live. An influence apparatus on the Spamouflage pattern works United States, allied, and diaspora audiences. Espionage, not extortion, carries the China-nexus loss: the prize is the firm's intellectual property and its communications.

Energy, communications, transport, water, the technology and semiconductor base, logistics, and finance each sit on a China targeting line. A firm gets selected through its sector, its region, or a carrier dependency, not through any China business of its own. The score holds at 89 (Likely, 75 percent), clear of any tier line. The read is collection and positioning, not effect. Taiwan pressure normalizes below the large-exercise threshold — the Eastern Theater Command ran four combat-readiness patrols in May 2026 without a Joint Sword-class exercise.

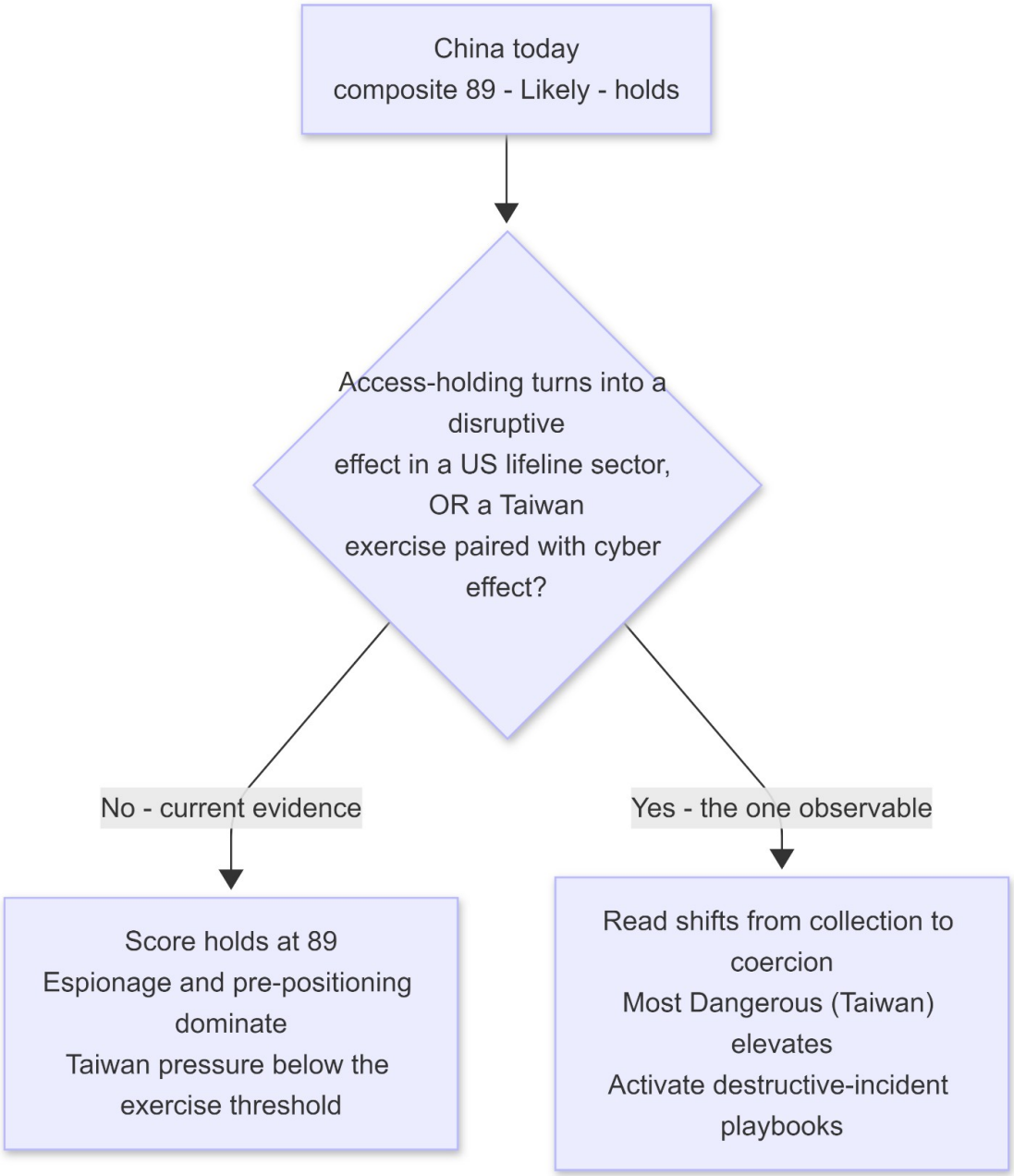


Figure C1. China — the one observable.

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

Russia — the strategic read

TL;DR. Russia holds 85 in the top tier, inside the 75–85 boundary review zone, so the score carries a standing senior-analyst review at the tier line. The GRU, FSB, and 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. The score holds at 85 through the October 13 resolution (Likely). One change moves the picture — quiet access turning into a disruptive effect inside a Western lifeline sector — and current evidence shows no such turn.

Russia ranks second in the field at 85, behind China and above North Korea 79 and Iran 78. Energy, telecommunications, transport, finance, and the defense supply base sit under pressure, with Ukraine and NATO Europe primary and an expanding line into Africa. A firm gets selected through its sector or its footprint, not through any direct quarrel with Moscow, and a supplier inside a lifeline sector carries the same exposure as the operator it supplies.

Russia runs three reinforcing operations: quiet intrusion into Western lifeline infrastructure through network edge devices, denial-of-service against allied government and logistics targets, and an influence push directed at the European governments now funding Ukraine. Energy, telecommunications, transport, finance, and the defense supply base sit under pressure. A firm gets selected through its sector or its footprint, not through any direct quarrel with Moscow. A supplier inside a lifeline sector carries the same exposure as the operator it supplies.

The score holds at 85 (Likely, 70 percent), inside the 75–85 boundary review zone, so the chapter carries a standing senior-analyst review at the tier line. United States support to Ukraine draws down, and targeting shifts toward the European funders; Sweden votes September 13, 2026, just past the horizon, and the influence line elevates around that window. France’s 2027 cycle sits next on the calendar.

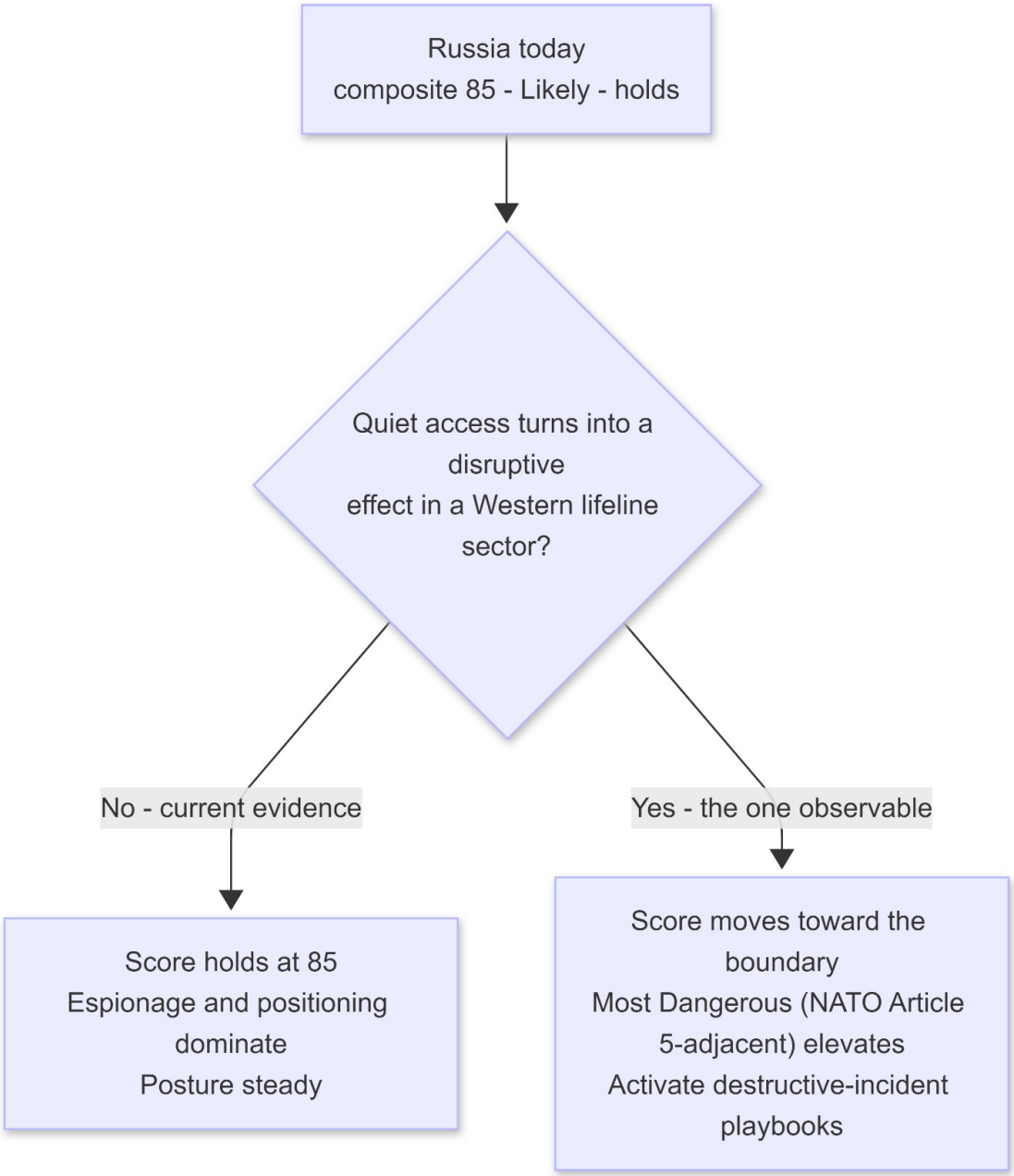


Figure C2. Russia — the one observable.

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 as a position and unlikely as an outcome, while the achieved path rates a protracted, grinding conflict under sanctions strain (Likely).

North Korea — the strategic read

TL;DR. North Korea holds 79 at the Tier 1 upper band, inside the boundary review zone, so the score carries senior-analyst review at the tier line. 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. The score holds at 79 through the October 13 resolution (Likely). One change moves the picture — revenue theft turning toward a destructive effect, or a capability jump through the Russia partnership — and current evidence shows no such turn.

Full BLUF. North Korea ranks third in the field at 79, above Iran 78 and below China and Russia. 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 United States companies, many in the Fortune 500. The cryptocurrency sector, financial technology, remote-hire employers, and the defense-industrial base each sit on a North Korea targeting line, the revenue engine running at tempo.

North Korea runs the most revenue-driven operation of the four. Three lines run together: cryptocurrency theft at state scale, fraudulent IT-worker placement inside Western firms, and espionage against defense, cryptocurrency, and blockchain targets. The Reconnaissance General Bureau directs the cyber units, the Lazarus Group among them. 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 United States companies, many in the Fortune 500.

The score holds at 79 (Likely, 72 percent), at the Tier 1 upper band inside the boundary review zone, so the score carries senior-analyst review at the tier line. The revenue engine runs at tempo. The share of global hack value has accelerated rather than plateaued, from below 10 percent in 2020 to 76 percent through April 2026.

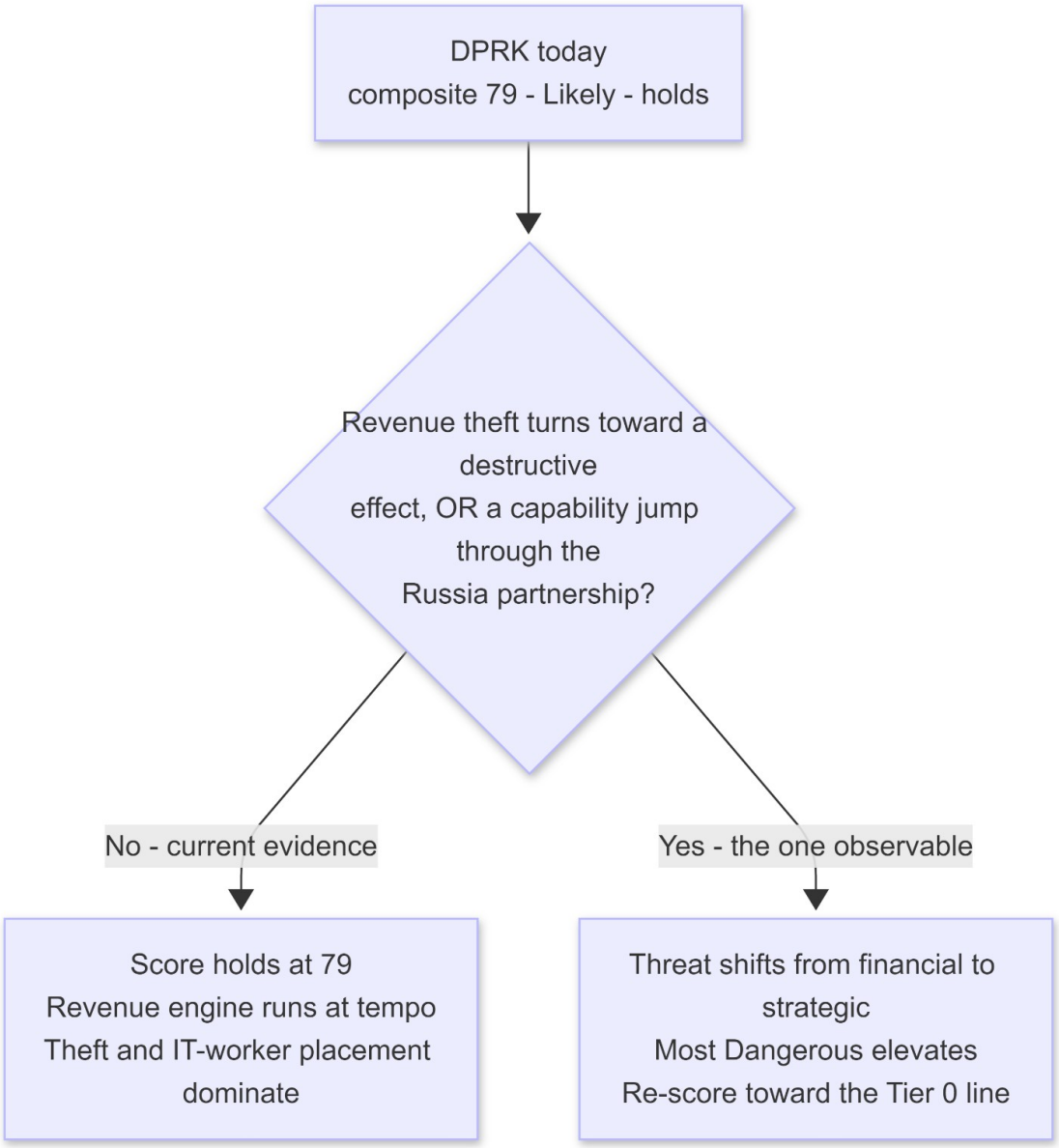


Figure C3. North Korea — the one observable.

Across the strategic horizon the triple endgame governs. The Most Likely course holds the composite in the 77–81 band with revenue theft sustained and the IT-worker program persistent. The Most Dangerous course runs a shift from theft toward a destructive effect, or a capability transfer through the Russia partnership. The tail runs a succession or regime shock that disrupts the operator pipeline.

Iran — the strategic read

TL;DR. Iran holds 78 at the Tier 1 upper band, inside the boundary review zone, so the score carries senior-analyst review at the tier line. The Islamic Revolutionary Guard Corps and the Ministry of Intelligence and Security 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. The score holds at 78 through the October 13 resolution (Likely). One change moves the picture — a renewed Israel or United States kinetic exchange that lifts the disruptive operational-technology line within days — and current evidence shows no such exchange.

Full BLUF. Iran ranks fourth among the Big Four at 78, the lowest of the set and still inside Tier 1. 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, the United States and Israel primary and Gulf hosts elevated. Iranian tempo tracks the kinetic cycle, so exposure runs episodic rather than steady, and the reported death of Supreme Leader Khamenei on February 28, 2026 and the unresolved succession sit as the central wildcard.

Iran runs three operational lines that rise with regional conflict: disruptive operations against operational technology — the industrial control systems behind water, energy, and fuel — espionage and surveillance against dissidents and policy targets, and influence operations augmented with artificial intelligence. The Islamic Revolutionary Guard Corps and the Ministry of Intelligence and Security direct the clusters. Iranian cyber tempo tracks the kinetic cycle, so an escalation raises the disruptive line within days and a sustained de-escalation lowers it.

The score moved to 78 this cycle (Likely, 70 percent), inside the boundary review zone, so the score carries senior-analyst review at the tier line. The move prices the espionage-to-destruction crossing: a destructive wiper deployment in March 2026 and IRGC-linked activity against United States water and energy systems. Supreme Leader Ali Khamenei was assassinated in February 2026, and Iran’s Assembly of Experts has since elected his son Mojtaba Khamenei, age 56, as the new Supreme Leader (corroborated by Iranian state media and multiple international outlets; ASA B2). The succession is resolved; the central wildcard is now the consolidation of the new leadership and any factional fallout that reshapes the operator pipeline.

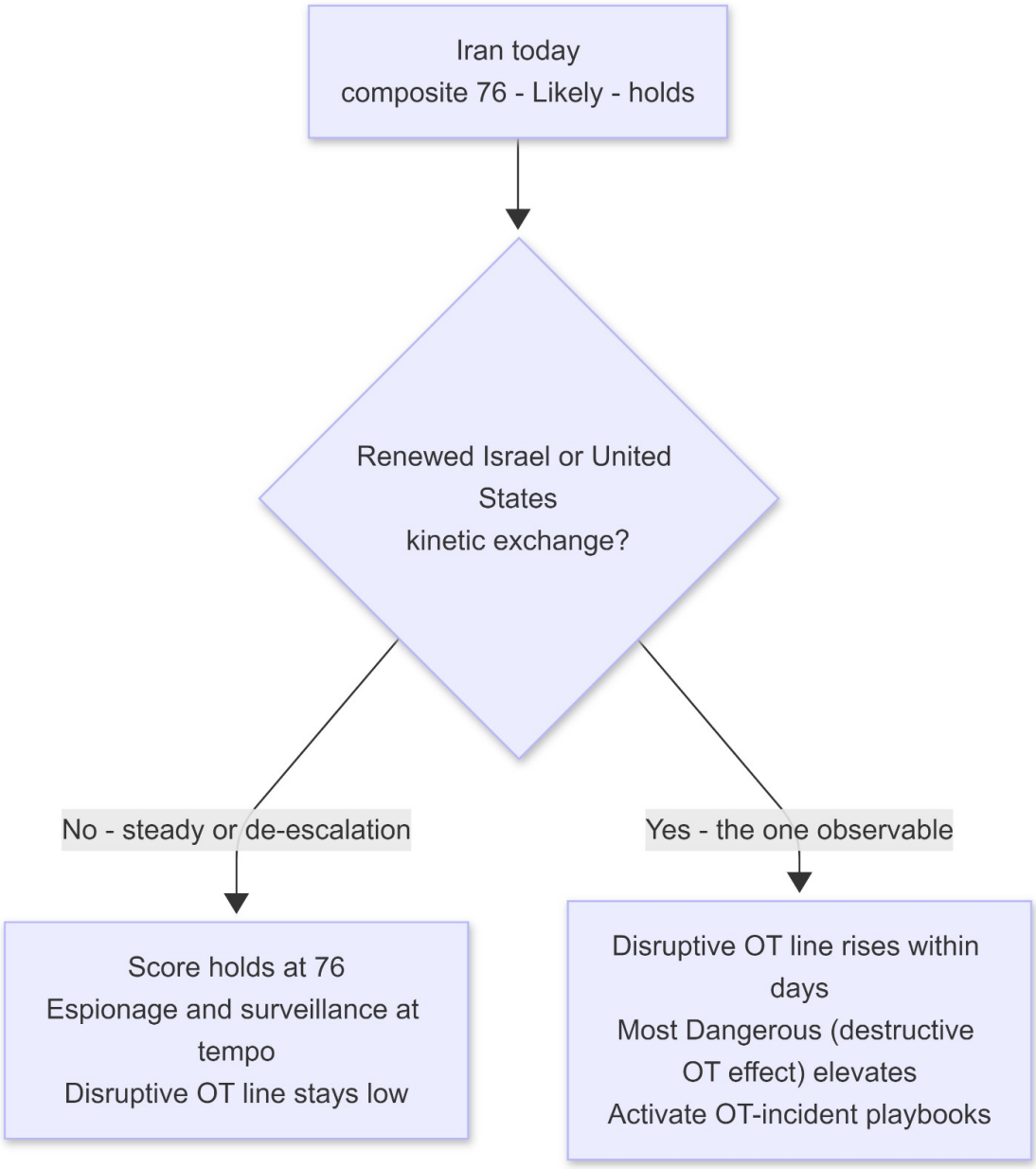


Figure C4. Iran — the one observable.

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

Recommendations and opportunities — board

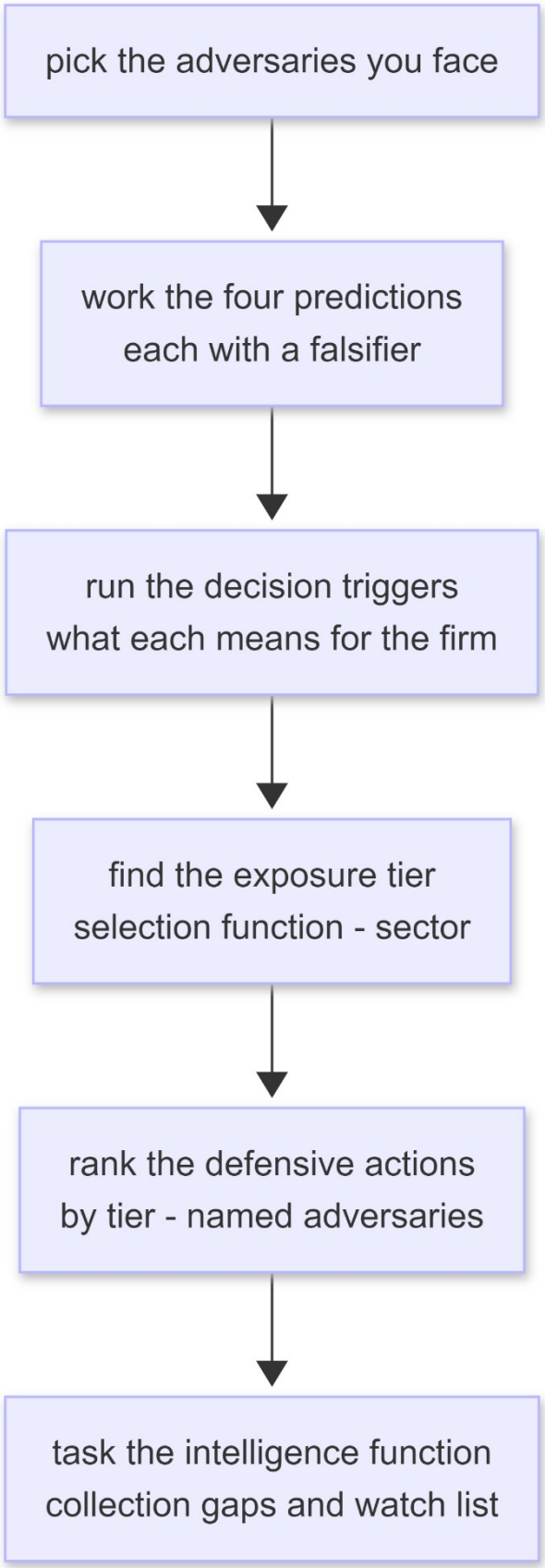
Four moves carry the board response across the portfolio. Each names why it matters, the risk it removes as a planning estimate, and a rough time to first value. The Operational tearline carries the effort, the completion tests, and the named adversary clusters. The estimates size

the cut for a firm exposed mainly through the named line; the real reduction depends on the environment.

Board move	Why it matters	Risk it removes (planning read)	Time to first value
Fund edge-device and identity hardening first	One spend answers the Chinese pre-positioning (Volt Typhoon, MSS) and the Russian intrusion line (APT28, APT44) at once, because the two break in through the same equipment; 40 percent of China-nexus exploited vulnerabilities in 2025 hit the network edge	A 50 to 80 percent cut to state-line initial access for a firm exposed mainly on that vector; covers two adversaries	2–6 weeks on the named appliance classes; identity controls across 1–2 quarters
Protect communications, intellectual property, and cryptocurrency custody	The China-nexus loss is collection, the North Korean loss is theft; each targets the crown jewels and the credentials	Cuts carrier-network and intellectual-property exposure and hardens cryptocurrency and credential custody	1–2 quarters
Screen the remote-hire and supplier pipeline	North Korea placed operatives inside more than 100 firms; the same screening answers the Chinese insider convergence and the Russian supply-chain line	Closes the insider and trusted-path routes that bypass perimeter controls	About 1 quarter
Set the four observables as board triggers	Each adversary carries one signal that changes its read; the firm acts on a named observable rather than a headline	Buys early warning; avoids over-reaction and under-reaction alike	Immediate once the watch is assigned

Opportunity	What the board gains
One scored axis	A single defensible metric for resource allocation and reporting, in place of vendor catalogs that resist comparison
Convergence coverage	Edge and identity hardening answers China and Russia together; insider screening answers North Korea and the Chinese tech-sector line at once
Mechanical escalation	Each board trigger ties to a named observable, so posture moves on a signal

Opportunity	What the board gains
	rather than a debate


pick the adversaries you face
work the four predictions each with a falsifier
run the decision triggers what each means for the firm
find the exposure tier selection function - sector
rank the defensive actions by tier - named adversaries
task the intelligence function collection gaps and watch list

TEARLINE 2 — OPERATIONAL

For risk, governance, security leadership, and the intelligence function

How to use the tearline. For each adversary the firm faces, work the four predictions as planning assumptions and stand a watch on every falsifier, read the decision triggers for what each means for the firm, find the exposure tier through the selection function, and assign the ranked actions to named owners with the horizon as the deadline. Task the intelligence function with the collection gaps. A firm facing more than one adversary reads the convergence note at the close. The flow below shows the path.

Figure D. Operational reader path.

China — operational

China holds the Tier 0 composite at 89, the catalog lead, outside the boundary review zone. The Ministry of State Security and its contractor ecosystem run APT41, APT31, APT40, and APT10; the People's Liberation Army runs military cyber under the 2024 reorganization that stood up the Information Support Force, the Cyberspace Force, and the Aerospace Force. Three lines run in parallel: pre-positioning inside United States lifeline infrastructure on the Volt Typhoon pattern, backbone and technology-sector espionage on the Salt Typhoon and MSS patterns, and AI-augmented influence on the Spamouflage pattern. The positioning line runs slow and patient, holding access for years; the espionage line runs at sustained high tempo; the influence line runs continuously in standard China working hours.

The operations cross cyber, information, economic, and physical exposure. Lifeline pre-positioning places communications, energy, transport, and water at risk during a Taiwan window. Backbone espionage exposes communications at population scale. Technology-sector collection feeds Beijing's AI and semiconductor programs under export-control pressure.

Prediction	Most-likely line	Kent / ASA	Base → adjusted	Competing alternative	Falsifier
CN-P1 · Target set	Telecom and backbone operators; technology and AI firms; lifeline edge-device operators	Likely / B2	Moderate → 76%	Pivot to cloud and identity vectors	Access moves off edge devices (IoC-5)
CN-P2 · Verticals	Technology, telecom, government, energy-water-transport, logistics; finance elevated	Likely / B2	Moderate → 74%	Concentration narrows to technology alone	New sector named (IoC-3/11)
CN-P3 ·	United States	Likely / B2	Low-	Footprint	No new-

Prediction	Most-likely line	Kent / ASA	Base → adjusted	Competing alternative	Falsifier
Geography	primary; Indo-Pacific allies elevated; 80-country telecom footprint persists		moderate → 70%	contracts under hardening	region telemetry by mid-horizon (IoC-12/16)
CN-P4 · Geopolitical	Collection-and-positioning frame holds; coercion below the armed-conflict threshold	Likely / B3	Moderate → 72%	Shift to active coercion on a Taiwan timeline	Access-to-effect transition in a lifeline sector (IoC-2)

Prediction	What it means for an exposed firm	Action through the horizon	If the falsifier fires
CN-P1 · Target set	State-grade collection pressure, not commodity crime	Hold edge, identity, and cloud trust paths to state-actor assumptions	Re-score against supply-chain and identity vectors
CN-P2 · Verticals	Sector membership alone selects a firm	Fund the ranked actions matched to the sector tier	Treat the newly named sector as elevated and re-run the selection function
CN-P3 · Geography	United States and Indo-Pacific operations raise exposure; the telecom footprint keeps communications exposure global	Weight third-party and site reviews by geography; review carrier dependencies	Extend monitoring to the new region ahead of reporting
CN-P4 · Geopolitical	Espionage and positioning dominate; disruption stays below the base case	Prioritize detection of quiet persistence	Activate destructive-incident playbooks and assume a Taiwan-timeline shift

Collection gap	Prediction bounded	Collection requirement
Depth of residual access inside United States carrier networks	Who, Geography	Carrier-network forensics (government-grade); congressional oversight record (commercial)

Collection gap	Prediction bounded	Collection requirement
PLA cyber order of battle after the 2024 reorganization	Who	Doctrine reporting (commercial); unit and procurement detail (government-grade)
Direction link between MSS contractors and the inauthentic-network operators	Who, Geopolitical	Platform takedown reporting (commercial); contractor-leak analysis (specialist)
Intent-versus-capability split on a Taiwan timeline	Geopolitical	Exercise tracking (commercial); leadership-signal collection (government-grade)

Watch item	Earliest observable	Cadence
Access moves off edge devices (IoC-5)	Advisory or vendor reporting naming supply-chain or identity as the lead vector	Monthly
New sector enters the target list (IoC-3/11)	A sector outside the named set in quarterly reporting	Monthly
Regional telemetry stalls (IoC-12/16)	No fresh regional disclosure by mid-horizon	Mid-horizon checkpoint
Access-to-effect transition (IoC-2)	First confirmed disruptive effect in a United States lifeline sector	Continuous
Taiwan blockade or quarantine escalation	Sustained interdiction posture after a large-scale exercise	Weekly

Sub-index	Score	Sub-index	Score
Cognitive Warfare Velocity	92	Sectoral Targeting Concentration	88
OPSEC Sophistication	92	AI Tradecraft Adoption	88
Adaptation	82	Doctrinal Maturity	89
Narrative Volume	90	Operational Tempo	88

Tri-score: T-Mature, D-Elevated, F-Likely. Cultural Nexus seven-dimension average 88.9 (Information Control 97 ceiling, Surveillance Reach 95, Symbolic Demonstration 94); Frame A delta minus 6, a stable, slow-surprising sovereign authoritarian profile. Course of action: Most Likely 75 percent holds the 87–91 band; Most Dangerous 15 percent runs a Taiwan escalation; the tail 10 percent runs economic disruption.

A commercial consumer reads the forecast through the selection function. The function asks a short set of yes-or-no questions, returns the China-nexus lines that select the firm, and sets an exposure tier from the count and severity of the lines that fire (Severe, High, Elevated, Moderate, Low).

Condition (IF)	China-nexus selecting line	Example entity
Operates or supplies a United States 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	An MSP, 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

Commercial sector	Selecting lines	Exposure tier
Technology, software, semiconductors, AI	Espionage, access-multiplier, supply-chain	High
Telecommunications and carriers	Backbone espionage, pre-positioning	High
Energy, water, transport	Pre-positioning	High
Defense-industrial base	Espionage, pre-positioning, supply-chain	High
Logistics, advanced manufacturing, finance	Espionage, access-multiplier	Elevated

The China-nexus picture differs from the Russian one: extortion is not the lead concern, so segmented recovery matters less than intellectual-property segmentation, insider screening, and communications protection.

Rank	Action	Defeats	Why it cuts risk (planning estimate)	Effort and time	Done when
1	Edge-device and identity hardening, living-off-the-land hunts	Volt Typhoon; MSS clusters	Closes the leading access path — 40 percent of 2025 China-nexus exploited vulnerabilities hit the edge, 67 percent granted immediate access; a 50–80 percent cut to state-line initial	Moderate; 2–6 weeks edge, 1–2 quarters identity	Appliances patched; hunt run; phishing-resistant identity on privileged access

Rank	Action	Defeats	Why it cuts risk (planning estimate)	Effort and time	Done when
			access		
2	Move sensitive traffic off carrier channels to end-to-end encryption	Salt Typhoon backbone espionage	Removes population-scale carrier exposure the index rates still live	Moderate; about 1 quarter	Sensitive traffic on independent end-to-end encryption; carrier dependencies inventoried
3	Intellectual-property segmentation and insider screening	MSS tech-sector collection; DPRK insider convergence	Protects the crown jewels that carry the loss	Moderate to High; 1–2 quarters	Crown-jewel data segmented; insider screening on sensitive roles
4	Supplier and managed-service review	Access-multiplier, relay masking	Removes trusted-path blind spots	Moderate; about 1 quarter	Trusted-path inventory complete; high-privilege third-party access re-authorized
5	Brand and narrative monitoring, pre-drafted response	Spamouflage influence	Cuts time-to-rebuttal	Low; 2–3 weeks	Watch live; rebuttal language approved in advance

Russia — operational

Russia holds the Tier 0 composite at 85, inside the 75–85 boundary review zone, so the chapter carries a standing senior-analyst review at the tier line. Three Russian services direct the state operations: the GRU runs APT28 (Forest Blizzard) and APT44 (Sandworm); the FSB runs Energetic Bear and Gamaredon (Aqua Blizzard); the SVR runs APT29 (Midnight Blizzard). A crowdsourced hacktivist project — NoName057(16) and the DDoSia project — runs the disruption; Doppelganger, Storm-1516, and Matryoshka run the influence. Three lines run in parallel: GRU intrusion and pre-positioning against NATO-aligned government, logistics, and energy targets; hacktivist-front denial-of-service over a state-tolerated criminal ecosystem; and an AI-augmented influence operation working the Western election calendar.

The work maps to programs a risk owner already runs: edge-device exposure management, identity controls, denial-of-service resilience, segmented and tested recovery, supplier review, and election-period narrative monitoring. Sector membership alone selects a firm; direct Russia exposure stays optional.

Prediction	Most-likely line	Kent / ASA	Base → adjusted	Competing alternative	Falsifier
RU-P1 · Target set	NATO-aligned government, logistics, telecom; Western energy edge-device operators	Likely / B2	Moderate → 75%	Pivot to direct-operator access	Access moves off edge devices (IoC-5)
RU-P2 · Verticals	Government, energy, transport, telecom, finance; media around elections	Likely / B2	Moderate → 72%	Expansion into a new sector	New sector named (IoC-11)
RU-P3 · Geography	Ukraine and NATO Europe; Western energy; Africa expanding	Likely / B2	Low-moderate → 70%	Allied infrastructure outside Europe drawn in	Telemetry in a new region (IoC-12/16)
RU-P4 · Geopolitical	Degrade Western funding will; below-threshold coercion; signaling	Likely / B3	Moderate → 68%	Shift to active coercion on a confrontation timeline	Access-to-effect transition in a lifeline sector (IoC-2)

Prediction	What it means for an exposed firm	Action through the horizon	If the falsifier fires
RU-P1 · Target set	State-grade intrusion pressure through the network edge	Inventory and harden internet-facing appliances; enforce identity controls	Re-score against direct-operator and identity vectors
RU-P2 · Verticals	Sector membership selects a firm	Fund the ranked actions matched to the sector tier	Treat the newly named sector as elevated and re-run the selection function
RU-P3 · Geography	NATO Europe and Ukraine-adjacent operations raise exposure	Weight reviews by geography; review energy and logistics dependencies	Extend monitoring outside Europe ahead of reporting
RU-P4 · Geopolitical	Below-threshold	Prioritize resilience	Activate destructive-

Prediction	What it means for an exposed firm	Action through the horizon	If the falsifier fires
	coercion dominates; disruption stays the worse case	and warning over disruption-only planning	incident playbooks; move the score toward the boundary

Collection gap	Prediction bounded	Collection requirement
Access-to-effect transition in a lifeline sector	Geopolitical	Operator and government disclosure (commercial); lifeline forensics (government-grade)
Newly named target sector	Verticals	Vendor quarterly reporting (commercial)
Africa expansion of the intrusion and influence lines	Geography	Regional telemetry and takedown reporting (commercial)
Direction link between the services and the hacktivist fronts	Who	Telegram tasking analysis (specialist); platform takedown reporting (commercial)

Watch item	Earliest observable	Cadence
Access moves off edge devices (IoC-5)	Advisory or vendor reporting naming a new lead vector	Monthly
New sector enters the target list (IoC-11)	A sector outside the named set in quarterly reporting	Monthly
Regional telemetry in a new region (IoC-12/16)	Fresh disclosure of activity outside Europe and Ukraine	Mid-horizon checkpoint
Access-to-effect transition (IoC-2)	First confirmed disruptive effect in a Western lifeline sector	Continuous
Election-period influence surge	Coordinated-inauthentic-behavior takedowns around the Swedish window	Weekly

Sub-index	Score	Sub-index	Score
Doctrinal Maturity	90	OPSEC Sophistication	85
Narrative Volume	89	AI Tradecraft Adoption	82
Cognitive Warfare Velocity	88	Sectoral Targeting Concentration	80
Operational Tempo	87	Adaptation	78

Tri-score: T-Mature, D-Elevated, F-Likely. Cultural Nexus seven-dimension average 83.3 (Symbolic Demonstration 95, Information Control 92, Resistance Ethos 88); Frame A delta minus 5, a stable, slow-adapting profile under managed elite strain. Course of action: Most

Likely 70 percent holds the boundary zone; Most Dangerous 20 percent runs a NATO Article 5-adjacent operation; the tail 10 percent runs internal disruption.

Condition (IF)	Russia-nexus 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	An MSP, cloud, or software provider
Is ransom-capable or uptime-sensitive	State-tolerated ransomware ecosystem	A manufacturer, healthcare provider, or service firm
Is election-adjacent or policy-facing	Doppelganger and Storm-1516 influence	A media outlet, party body, or policy organization

Commercial sector	Selecting lines	Exposure tier
Energy, telecom, transport (lifeline)	Pre-positioning, hacktivist disruption	High to Severe
Government and logistics	Hacktivist disruption, espionage	High
Defense supply base	Espionage, supply-chain	High
Finance, healthcare, media	Criminal-nexus, influence	Elevated
Professional services	Criminal-nexus	Moderate

The Russia-based ransomware ecosystem operates from Russian territory with state tolerance rather than state direction (posture flag: state-tolerated; ASA B3). For a firm with no European or lifeline exposure, it is the single largest Russia-nexus risk, answered through segmented, tested recovery rather than the state-line controls.

Rank	Action	Defeats	Why it cuts risk (planning estimate)	Effort and time	Done when
1	Edge-device and identity hardening, living-off-the-land hunts	APT28, APT44, APT29	A 50–80 percent cut to state-line initial access; converges with the China hardening spend	Moderate; 2–6 weeks edge, 1–2 quarters identity	Appliances patched; hunt run; identity enforced
2	Denial-of-service resilience and rehearsed response	NoName057(16), DDoSia	Cuts outage duration and the look of disorder	Moderate; about 1 quarter	Upstream scrubbing in place; response rehearsed

Rank	Action	Defeats	Why it cuts risk (planning estimate)	Effort and time	Done when
3	Segmented, tested backup and recovery	State-tolerated ransomware ecosystem	Removes the single largest risk for non-lifeline firms	Moderate to High; 1–2 quarters	Backups offline and restore-tested
4	Supplier and managed-service review	APT29 supply-chain access	Closes the access-multiplier route	Moderate; about 1 quarter	Trusted-path inventory complete
5	Election-period narrative monitoring, pre-drafted response	Doppelgange r, Storm-1516	Cuts time-to-rebuttal around the September window	Low; 2–3 weeks	Watch live; rebuttal approved in advance

North Korea — operational

The DPRK holds the Tier 1 composite at 79, at the upper band inside the boundary review zone, so the score carries senior-analyst review at the tier line. The Reconnaissance General Bureau directs the cyber program; the Lazarus Group and its TraderTraitor subset run the cryptocurrency thefts, and the IT-worker program runs thousands of placed operatives through stolen identities, United States-based facilitators, and laptop farms. Three lines run together: cryptocurrency theft at state scale, fraudulent IT-worker placement, and espionage against defense, cryptocurrency, and blockchain targets — the Mach-O Man campaign turns routine business communication into credential theft against executives.

The operations carry financial, data, and insider exposure rather than physical risk. The cryptocurrency line drains the cryptocurrency sector at scale and funds the weapons program. The IT-worker line plants hostile insiders, creating remediation cost, legal exposure, and data-theft risk from trusted accounts. Revenue is the strategic point: sanctions make cybercrime a primary funding source, so the operation runs as state policy.

Prediction	Most-likely line	Kent / ASA	Base → adjusted	Competing alternative	Falsifier
KP-P1 · Target set	Crypto exchanges, DeFi and bridge protocols and executives; remote-hire employers; defense and aerospace	Likely / B2	Moderate → 78%	Pivot to traditional finance as custody hardens	Revenue model moves off crypto and IT-worker fraud (IoC-5)
KP-P2 · Verticals	Cryptocurren cy and DeFi;	Likely / B2	Moderate → 75%	Concentratio n narrows to	New sector named (IoC-

Prediction	Most-likely line	Kent / ASA	Base → adjusted	Competing alternative	Falsifier
	financial technology; remote-hire employers; defense and aerospace			cryptocurrency alone	3/11)
KP-P3 · Geography	United States primary for IT-worker fraud; global crypto sector; South Korea and Japan elevated	Likely / B2	Low-moderate → 72%	Footprint narrows under coordinated enforcement	No new-region telemetry by mid-horizon (IoC-12/16)
KP-P4 · Geopolitical	Revenue-generation frame holds; theft funds the regime and the weapons program	Likely / B2	Moderate → 76%	Shift toward destructive or disruptive strategic use	Move from theft to destructive effect (IoC-2)

Prediction	What it means for an exposed firm	Action through the horizon	If the falsifier fires
KP-P1 · Target set	Crypto holders and remote-hire employers face state-grade theft and insider placement	Harden custody and cryptographic-material handling; screen remote-hire identity; treat outreach as hostile	Re-score against the new revenue vector
KP-P2 · Verticals	Sector membership selects a firm; the crypto and remote-hire lines carry direct loss	Fund the ranked actions matched to the sector tier	Treat the newly named sector as elevated and re-run the selection function
KP-P3 · Geography	United States remote-hire exposure and global crypto exposure run in parallel	Weight identity screening to United States hiring; treat crypto exposure as geography-independent	Extend monitoring to the new region ahead of reporting
KP-P4 · Geopolitical	The threat is financial, not destructive	Prioritize asset protection and fraud detection over destructive-incident planning	Activate destructive-incident playbooks and reassess as a strategic threat

Collection gap	Prediction bounded	Collection requirement
Attribution split between Lazarus and newer subgroups	Who	Blockchain-intelligence attribution (commercial); on-chain laundering analysis (specialist)
Scale of active IT-worker placements after enforcement	Who, Verticals	DOJ and FBI enforcement records (commercial); remote-hire fraud telemetry (commercial)
Depth of the Russia capability and sanctions-evasion channel	Geopolitical	Leadership-signal collection (government-grade); sanctions-monitoring reporting (commercial)
Laundering-infrastructure resilience under interdiction	Who, Geopolitical	Cross-chain bridge monitoring (commercial); exchange compliance reporting (commercial)

Watch item	Earliest observable	Cadence
Revenue model moves off crypto and IT-worker fraud (IoC-5)	Reporting naming a new primary revenue vector	Monthly
New sector enters the target list (IoC-3/11)	A sector outside the named set in quarterly reporting	Monthly
Shift from theft to destructive effect (IoC-2)	First confirmed destructive operation against a non-financial target	Continuous
Major Russia capability or technology transfer	Disclosed transfer; a step-change in tradecraft	Weekly
Laundering-infrastructure takedown	Multi-jurisdiction seizure; bridge or mixer shutdown	Weekly

Sub-index	Score	Sub-index	Score
OPSEC Sophistication	80	Sectoral Targeting Concentration	78
Operational Tempo	78	Doctrinal Maturity	75
Narrative Volume	72	Adaptation/ Evolution Index	71
Cognitive Warfare Velocity	65	AI Tradecraft Adoption	65

Tri-score: T-Mature, D-Operational, F-Mature — the highest forecast confidence among the Big Four, because the revenue engine is consistent and well-instrumented through on-chain telemetry. Cultural Nexus seven-dimension average near 86, the catalog's most extreme bimodal profile: Information Control and Symbolic Demonstration at 100, against Technology Adoption at 23, the catalog floor. Course of action: Most Likely holds the 77–81 band; Most

Dangerous runs a shift from theft to destructive effect or a Russia-enabled capability jump; the tail runs a succession or regime shock.

Condition (IF)	DPRK-nexus 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 (Mach-O Man)	A fintech, wallet, or blockchain provider
Is a defense or aerospace contractor	Espionage against weapons-relevant technology	A defense-industrial-base supplier
Is ransom-capable or uptime-sensitive	Financially motivated intrusion; revenue substitutes for extortion	A manufacturer, healthcare provider, or service firm

Commercial sector	Selecting lines	Exposure tier
Cryptocurrency exchanges and custodians	State-scale theft; executive social engineering	High
Decentralized finance, bridges, and protocols	State-scale theft; multisig and bridge compromise	High
Financial technology and payments	Theft; executive-targeted social engineering	High
Any firm hiring remote technical staff	Fraudulent IT-worker placement; insider risk	High
Defense and aerospace; blockchain infrastructure	Weapons-relevant espionage; supply-chain	Elevated

The DPRK-nexus criminal line reads state-directed, the clearest case among the Big Four. The RGB directs the theft, and the proceeds fund the regime rather than private enrichment. For most private firms the concern is direct financial loss and hostile insider placement rather than espionage or disruption. The deception discount applies only to the regime's denials, not to the documented operations (Highly likely; corroborated; ASA B2).

Rank	Action	Defeats	Why it cuts risk (planning estimate)	Effort and time	Done when
1	Custody, cryptographic-material, and multisig and bridge governance hardening	Lazarus, TraderTraitor theft	Closes the route behind 76 percent of 2026 global crypto-hack value	Moderate to High; 1–2 quarters	Custody segmented; multisig and bridge governance reviewed; large transfers gated
2	Remote-hire	IT-worker	Closes the	Moderate;	Identity

Rank	Action	Defeats	Why it cuts risk (planning estimate)	Effort and time	Done when
	identity screening and laptop-farm detection	program	insider route that placed operatives inside 100-plus firms; converges with the China insider line	first pass 2–4 weeks	verification live; laptop-farm screening in the hiring pipeline
3	Executive and developer social-engineering defense	Mach-O Man espionage	Cuts the recruiter and investor entry pattern	Low; 2–3 weeks	High-value staff trained on the lure; device controls enforced
4	Insider-risk program for technical staff	Insider data and asset theft	Surfaces hostile-insider behavior earlier	Moderate; ongoing	Access scoped and logged; anomalous access reviewed
5	Asset-recovery and reporting readiness	Theft response	Speeds recovery and reporting after a theft	Moderate; about 1 quarter	Incident and recovery plan rehearsed; blockchain-intelligence alerting integrated

Iran — operational

Iran holds the Tier 1 composite at 78, inside the boundary review zone, so the score carries senior-analyst review at the tier line. The IRGC Intelligence Organization and the IRGC Cyber-Electronic Command run one track; the Ministry of Intelligence and Security runs the other. Attributed clusters include APT35 (Charming Kitten), APT42, APT34 (OilRig), APT39, MuddyWater, and the IRGC-CEC persona CyberAv3ngers. Three lines run together and rise with regional conflict: disruptive operations against operational technology, espionage and surveillance against dissidents and policy targets, and AI-augmented influence.

The operations split two ways for a private firm: physical disruption risk for control-system operators, and population-scale data exposure for data holders. Iranian tempo tracks the kinetic cycle, so exposure is episodic rather than steady.

Prediction	Most-likely line	Kent / ASA	Base → adjusted	Competing alternative	Falsifier
IR-P1 · Target set	Exposed industrial-	Likely / B2	Moderate → 74%	Collection narrows to	Access moves off exposed

Prediction	Most-likely line	Kent / ASA	Base → adjusted	Competing alternative	Falsifier
	control operators; dissident-data holders; government and policy bodies; conflict-exposed firms			surveillance-only between spikes	control devices and phishing (IoC-5)
IR-P2 · Verticals	Water-energy-fuel; telecom and data holders; government; media and human rights	Likely / B2	Moderate → 72%	Concentration narrows to operational technology alone	New sector named (IoC-3/11)
IR-P3 · Geography	United States and Israel primary; Gulf hosts elevated; Europe a standing target	Likely / B2	Low-moderate → 70%	Footprint contracts to Israel-only outside conflict	No new-region telemetry by mid-horizon (IoC-12/16)
IR-P4 · Geopolitical	Conflict-reactive, asymmetric, deniable; tempo tracks the kinetic cycle	Likely / B3	Moderate → 68%	Sustained campaign decoupled from kinetic events	Tempo holds steady through a de-escalation window (IoC-2)

Prediction	What it means for an exposed firm	Action through the horizon	If the falsifier fires
IR-P1 · Target set	Control-system operators and data holders face state-grade pressure, sharpest during conflict	Pull control devices off the public internet; harden identity against phishing; watch the kinetic calendar	Re-score against the new access vectors
IR-P2 · Verticals	Sector membership selects a firm; the water-energy-fuel line carries physical risk	Fund the ranked actions matched to the sector tier	Treat the newly named sector as elevated and re-run the selection function
IR-P3 · Geography	United States, Israeli, and Gulf-host operations raise	Weight site and third-party reviews by geography and the	Extend monitoring to the new region ahead

Prediction	What it means for an exposed firm	Action through the horizon	If the falsifier fires
	exposure during conflict windows	kinetic cycle	of reporting
IR-P4 · Geopolitical	Tempo tracks the kinetic cycle, so exposure is episodic	Tie monitoring posture to conflict events; pre-stage the destructive-incident response	Shift to steady-state defense; assume a decoupled, sustained campaign

Collection gap	Prediction bounded	Collection requirement
Depth of access inside compromised United States control-system networks	Who, Geography	Operational-technology forensics (government-grade); operator disclosure (commercial)
IRGC-CEC and MOIS contractor order of battle	Who	Sanctions and indictment records (commercial); contractor-leak analysis (specialist)
Direction link between the IRGC and the influence personas	Who, Geopolitical	Platform takedown reporting (commercial); academic forensic studies (commercial)
New-leadership (Mojtaba) effect on the operator pipeline	Geopolitical	Leadership-signal collection (government-grade); dissident and diaspora reporting (commercial)

Watch item	Earliest observable	Cadence
Access moves off exposed control devices and phishing (IoC-5)	Advisory or vendor reporting naming a new lead vector	Monthly
New sector enters the target list (IoC-3/11)	A sector outside the named set in quarterly reporting	Monthly
Tempo decouples from the kinetic cycle (IoC-2)	Sustained operations through a clear de-escalation window	Continuous
Renewed Israel or United States kinetic strike	Open conflict reporting; fast-reaction persona mobilization	Continuous
Mojtaba consolidation rupture	State-media anomaly; factional signaling; protest activation around the new leadership	Weekly

Sub-index	Score	Sub-index	Score
Cognitive Warfare Velocity	82	Sectoral Targeting Concentration	82

Sub-index	Score	Sub-index	Score
OPSEC Sophistication	84	AI Tradecraft Adoption	78
Narrative Volume	78	Operational Tempo	80
Doctrinal Maturity	70	Adaptation/ Evolution Index	70

Tri-score: T-Mature, D-Elevated, F-Likely. Cultural Nexus seven-dimension average near 84; Resistance Ethos at 94 stands as the highest dimension and the engine of operator motivation under sanctions. Frame A delta minus 6, a sovereign-state authoritarian profile under strain, with elite cohesion the soft dimension exposed by the succession question. Course of action: Most Likely holds the 76–80 band with conflict-tracked spikes; Most Dangerous runs a destructive operational-technology effect with physical consequence during a kinetic exchange; the tail runs a succession-driven internal disruption.

Condition (IF)	Iran-nexus 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 United States or Israeli facilities in the Gulf	Conflict-reactive targeting during kinetic windows	A firm with Gulf operations or base support
Carries a visible Israel or United States alignment	Influence and hack-and-leak targeting	A brand or institution publicly tied to either state

Commercial sector	Selecting lines	Exposure tier
Water, wastewater, and fuel systems	Operational-technology disruption; physical risk	High
Energy and utilities	Operational-technology disruption	High
Internet providers and telecommunications	Surveillance; population-scale data theft	High
Government, policy, and defense suppliers	Espionage and surveillance	High
Media, research, human rights; Gulf-host firms	Surveillance, influence; conflict-reactive targeting	Elevated

The Iran-nexus disruptive line reads state-directed: the IRGC-CEC directs CyberAv3ngers, confirmed through the United States Treasury designation of six IRGC-CEC officials, and the destructive operations carry ideological rather than profit motive. The deception discount applies only to the false claims and inflated hacktivist messaging, not to the documented operations (Highly likely; corroborated; ASA B2).

Rank	Action	Defeats	Why it cuts risk (planning estimate)	Effort and time	Done when
1	Pull industrial-control devices off the public internet; replace default credentials; segment operational-technology networks	CyberAv3ngers, IRGC-CEC disruption	Removes the disruptive-OT entry that rises within days of a kinetic exchange	Moderate to High; 1–2 quarters	No control device internet-reachable; default credentials replaced; segmentation verified
2	Phishing-resistant identity; treat outreach as hostile	APT35, APT42, MuddyWater espionage	Closes the espionage and surveillance entry vectors	Moderate; 2–6 weeks	Multifactor on all accounts; staff trained on the impersonation pattern
3	Personal-data segmentation and access control	MOIS and IRGC surveillance	Cuts the surveillance and intimidation route	Moderate; about 1 quarter	Crown-jewel data segmented; access logged and reviewed
4	Rehearsed destructive-incident response with offline backup	Destructive precedent	Converts the kinetic-cycle warning into a rehearsed response	Low to Moderate; continuous	Playbook rehearsed; backups offline and restore-tested
5	Narrative monitoring for false attack claims, pre-drafted response	Cotton Sandstorm, IRGC amplification	Separates real effect from claimed effect; cuts panic	Low; 2–3 weeks	Watch live; response language approved in advance

Field beyond the Big Four — cluster concentration and selection

The 38 actors below the Big Four concentrate within clusters and sectors, and the operational reader uses that concentration to set collection and control priority. The Salafi-jihadist cluster carries the largest count at 12 actors, with JNIM at 62 and ISKP at 61 at the top, and concentrates on government, military, and humanitarian targets across the Sahel and Central Asia. The Iranian Axis runs four mains plus seven component annexes, with the Houthi movement now first at 63, and concentrates on maritime, energy, and regional government targets. The gray-zone state-cyber cluster — Turkey, India, Qatar, Vietnam, the United Arab

Emirates, and Saudi Arabia between 48 and 53 — concentrates on espionage against regional rivals and diaspora communities.

Three financially driven groups read Tier 2 at 56 and matter for any firm with payment exposure: the Russian-speaking ransomware ecosystem, the Sinaloa Cartel at 54, and the Belarus and Africa Corps state-aligned successors. The ransomware ecosystem selects on payment capacity and reachability rather than on sector grievance, so a firm with no European or state exposure still carries that line. The hacktivist networks — NoName057(16) at 47 down to Anonymous Sudan at 21 — select on symbolic visibility and run denial-of-service against named events.

The selection logic holds across the field. A firm enters an adversary's set through sector, region, or a single dependency, not through any direct quarrel. The convergence that follows for the Big Four — one hardening program covering more than one state line — extends to the field: the edge-device and identity controls that answer Russian and Chinese pre-positioning also reduce the initial-access surface the ransomware ecosystem and the gray-zone cyber actors favor.

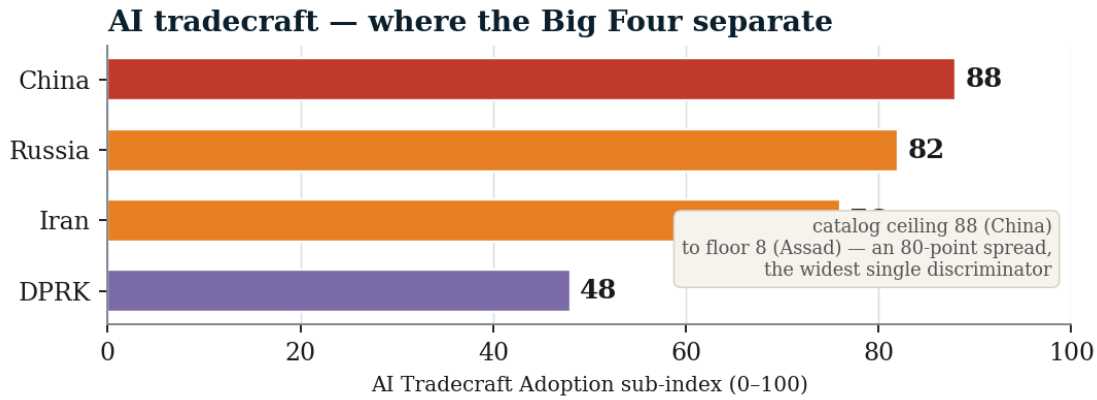


Figure A2. AI Tradecraft Adoption separates the Big Four more sharply than any other sub-index. The 80-point spread from the catalog ceiling at 88 to the floor at 8 is the widest single discriminator the index measures.

The full 42-actor field — ranked catalog and selection guide

The Big Four lead a catalog of 42 named adversaries plus seven Iranian-Axis component annexes. Below the four state powers, 38 actors hold tiered positions across nine operational clusters. The Houthi movement leads that field at 63 after the June 2026 Cluster 2 reconciliation, and the former Assad regime networks sit at the floor at 16. No actor below the Big Four reaches the peer-state band, so the four keep the deep treatment here while the field below them reads at catalog depth.

Depth note. The Big Four carry full operational and tactical treatment here. The 38 actors below them carry catalog placement, cluster concentration, and a selecting condition here; full operational and tactical depth for the 38 lives in the companion addendum one-pagers and deepens through the Tier 2 scoring cycle.

The split runs nine actors in Tier 1, 27 in Tier 2, and four in Tier 3 across the full catalog; among the 38 below the Big Four the same field reads seven, 27, and four. Seven hold Tier 1 below the Big Four — the Houthi movement at 63, JNIM at 62, Hezbollah and ISKP at 61, Pakistan's Inter-Services Intelligence at 60, and ISIS-Core and the Iraqi Resistance front groups at 59. The Salafi-jihadist cluster is the largest single group in the catalog at 12 actors. Belarus, Africa Corps, and the Russian-speaking ransomware ecosystem score 56 yet read Tier 2, because the published band draws the Tier 1 line in the score gap above them.

The reconciliation moved four Cluster 2 actors against indicator-level evidence. The Houthi movement rose from 57 to 63 on the Red Sea campaign and the Al-Masirah media operation. Hamas fell from a paired 60 to 54 under sustained command attrition and crossed from Tier 1 into Tier 2, while Palestinian Islamic Jihad split out at 46 as a Tier 2 component annex. Hezbollah corrected from an unsupported 64 to 61, and the Iraqi Resistance front groups moved from 58 to 59. The Houthi rise (plus 6) and the Hamas decline (minus 6) carry formal written justification and a senior-review hold.

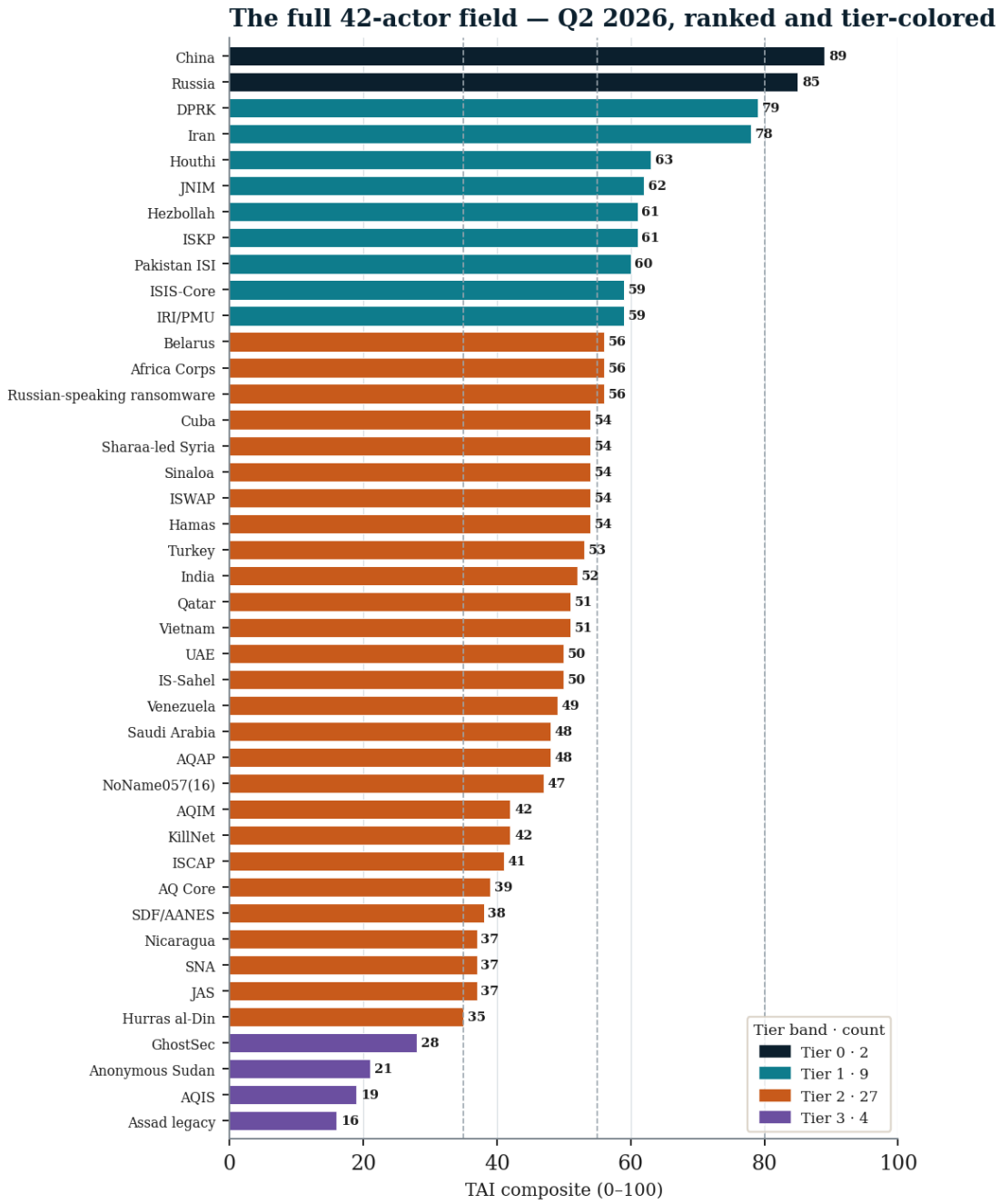


Figure B1. The full 42-actor field, ranked and colored by tier band. The dashed lines mark the Tier 3 to Tier 2 (35), Tier 2 to Tier 1 (55), and Tier 1 to Tier 0 (80) boundaries.

The reconciled catalog reads as follows. Cluster labels mark the operational grouping; the composite runs 0 to 100, and the tier follows the four-tier bands.

The ten clusters group the catalog by operational character: Cluster 1 Belarus and Wagner-successor structures, Cluster 2 the Iranian Axis of Resistance, Cluster 3 the ALBA bloc, Cluster 4 post-Assad Syrian factions, Cluster 5 Asian authoritarian intelligence services, Cluster 6 gray-

zone state cyber actors, Cluster 7 Salafi-jihadist networks, Cluster 8 cartels and paramilitary, Cluster 9 cybercrime ecosystems, and Cluster 10 hacktivist networks.

Cluster	Actor	Composite	Tier
Big Four	China	89	0
Big Four	Russia	85	0
Big Four	DPRK	79	1
Big Four	Iran	78	1
Cluster 2	Houthi movement	63	1
Cluster 7	JNIM	62	1
Cluster 2	Hezbollah	61	1
Cluster 7	ISKP	61	1
Cluster 5	Pakistan ISI	60	1
Cluster 7	ISIS-Core	59	1
Cluster 2	Iraqi Resistance IRI/PMU	59	1
Cluster 1	Belarus	56	2
Cluster 1	Africa Corps	56	2
Cluster 9	Russian-speaking ransomware	56	2
Cluster 3	Cuba	54	2
Cluster 4	Sharaa-led Syria	54	2
Cluster 8	Sinaloa Cartel	54	2
Cluster 7	ISWAP	54	2
Cluster 2	Hamas	54	2
Cluster 6	Turkey	53	2
Cluster 6	India	52	2
Cluster 6	Qatar	51	2
Cluster 6	Vietnam	51	2
Cluster 6	United Arab Emirates	50	2
Cluster 7	ISIS-Sahel	50	2
Cluster 3	Venezuela	49	2
Cluster 6	Saudi Arabia	48	2
Cluster 7	AQAP	48	2
Cluster 10	NoName057(16)	47	2
Cluster 7	AQIM	42	2
Cluster 10	KillNet	42	2
Cluster 7	ISCAP	41	2
Cluster 7	AQ Core	39	2
Cluster 4	AANES / SDF	38	2
Cluster 3	Nicaragua	37	2
Cluster 4	Syrian National	37	2

Cluster	Actor	Composite	Tier
	Army		
Cluster 7	JAS	37	2
Cluster 7	Hurras al-Din	35	2
Cluster 10	GhostSec	28	3
Cluster 10	Anonymous Sudan	21	3
Cluster 7	AQIS	19	3
Cluster 4	Former Assad regime legacy	16	3

Field selection guide — does a field actor select your firm

The catalog above ranks the field; the guide below makes the field actionable. A firm reads down the clusters its sector and region touch, finds the selecting condition, and matches the control that answers it. The control column points to the same converged actions the Big Four chapters carry, so one hardening program often answers a field actor and a state actor together. The guide runs the same selection logic as the Big Four IF tables — sector, region, and dependency decide whether an actor selects a firm — at catalog depth rather than per-actor depth. Depth for each named actor sits in the companion addendum one-pagers.

Cluster	**If your firm operates**	**Selecting actors (Tier band)**	**Control that answers it**
Cluster 2 — Iranian Axis	Maritime, shipping, Red Sea energy and trade; regional government	Houthi 63, Hezbollah 61, IRI/PMU 59	OT isolation and segmentation; destructive-incident response (same as Iran)
Cluster 7 — Salafi-jihadist	Government, military, NGO and humanitarian, extractive security in the Sahel and Central Asia	JNIM 62, ISKP 61, ISIS-Core 59	Physical-cyber convergence planning; staff and site security; narrative monitoring
Cluster 5 — Asian authoritarian	Firms with South Asia operations or rivalry exposure	Pakistan ISI 60	Edge and identity hardening; espionage-grade access control (same as China)
Cluster 1 — Belarus / Wagner-successor	NATO-Europe government and logistics; African extractive and security	Belarus 56, Africa Corps 56	Edge and identity hardening (same as Russia); regional dependency review
Cluster 9 — Cybercrime	Any ransom-capable or uptime-sensitive firm, regardless of sector	Russian-speaking ransomware 56	Segmented, restore-tested backups (same as Russia rank 3)
Cluster 8 — Cartels	Logistics, cross-border transport,	Sinaloa Cartel 54	Insider screening; physical-cyber

Cluster	If your firm operates	Selecting actors (Tier band)	Control that answers it
	firms with Mexico or border operations		convergence; supplier review
Cluster 6 — Gray-zone state cyber	Diaspora-facing media, regional rivals, firms in Gulf and South Asia	Turkey 53, India 52, Qatar/Vietnam 51, UAE 50, Saudi 48	Espionage-grade identity and data segmentation
Cluster 3 — ALBA bloc	Firms with Latin American government or critical-infrastructure exposure	Cuba 54, Venezuela 49, Nicaragua 37	Surveillance-aware data protection; regional access review
Cluster 10 — Hacktivist	Event-adjacent, symbolically visible, or publicly aligned brands	NoName057(16) 47, KillNet 42	Denial-of-service resilience; narrative monitoring (same as Russia/Iran)
Cluster 4 — Post-Assad Syria	Firms with Syria-adjacent or regional reconstruction exposure	Sharaa-led Syria 54, AANES/SDF 38	Standard access hardening; low active-threat posture (degraded cluster)

Multi-actor convergence

A firm that faces more than one of the four answers them together more cheaply than apart. On lifeline infrastructure, Chinese pre-positioning of the Volt Typhoon class and Russian positioning against Western energy converge on the same edge and identity equipment, so one hardening program covers the pair. On the technology sector, Chinese collection and the North Korean insider line run through people and access, so one insider-screening program covers the pair. On operational technology, the Iranian disruptive line shares the segmentation and offline-recovery controls that answer the destructive risk from any state actor. Election-period and conflict-period narrative monitoring carries across Russia and Iran. The convergence is the budgeting case: rank the actions once, against the union of the adversaries the firm faces, rather than once per adversary.

Convergence sizing. The table below puts numbers under the pairing claim. Each row names one control program, the adversaries one spend covers, and the planning-estimate risk cut for a firm exposed mainly on that vector. The estimates are environment-dependent planning figures, not guarantees, and they assume the firm carries the named exposure; a firm without that exposure reads its own row lower. The single-program cost lands well below the sum of the per-adversary programs, which is the budgeting case.

Control program	Adversaries one spend covers	Risk cut (planning estimate)	Why the spend converges
Edge-device and identity hardening, living-off-the-land hunts	China (Volt Typhoon, MSS), Russia (APT28, APT44, APT29), Pakistan ISI	50–80% cut to state-line initial access; closes the path behind ~40% of 2025 China-nexus	One program covers three state intrusion sets that break in through the same equipment

Control program	Adversaries one spend covers	Risk cut (planning estimate)	Why the spend converges
		exploited vulnerabilities	
Insider and remote-hire screening	North Korea (IT-worker program), China (MSS insider collection), Sinaloa Cartel	Closes the insider and trusted-path route that bypassed perimeter controls at 100-plus firms	One screening program covers the DPRK insider line and the Chinese insider-collection line
OT isolation, segmentation, offline-tested recovery	Iran (CyberAv3ngers, IRGC-CEC), any state destructive risk, Houthi field exposure	Removes the disruptive-OT entry that rises within days of a kinetic exchange	One OT program answers the Iranian disruptive line and the destructive risk from any state actor
Segmented, restore-tested backups	Russia-based ransomware ecosystem, North Korea destructive contingency	Removes the single largest risk for a non-lifeline firm; cuts ransom pressure	One recovery program answers extortion and destructive contingencies together
Election- and conflict-period narrative monitoring	Russia (Doppelganger, Storm-1516), Iran (Cotton Sandstorm), hacktivist fronts	Cuts time-to-rebuttal; separates real effect from claimed effect	One watch-and-response program covers the Russian and Iranian influence lines and the hacktivist field
Supplier and managed-service review	China (access-multiplier), Russia (APT29 supply-chain), field MSP exposure	Closes the trusted-path blind spot across state and field actors	One third-party program covers the supply-chain route every sophisticated actor favors

TEARLINE 3 — TACTICAL-TECHNICAL

For analysts, hunters, and detection engineers

How to use the tearline. 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. Seed the verification record so the September resolution stays mechanical. The index does not publish indicators or detection content — pull those from the threat-intelligence feed and read the tier for attribution, grading, and the falsifier-driven priorities. The flow below shows the path.

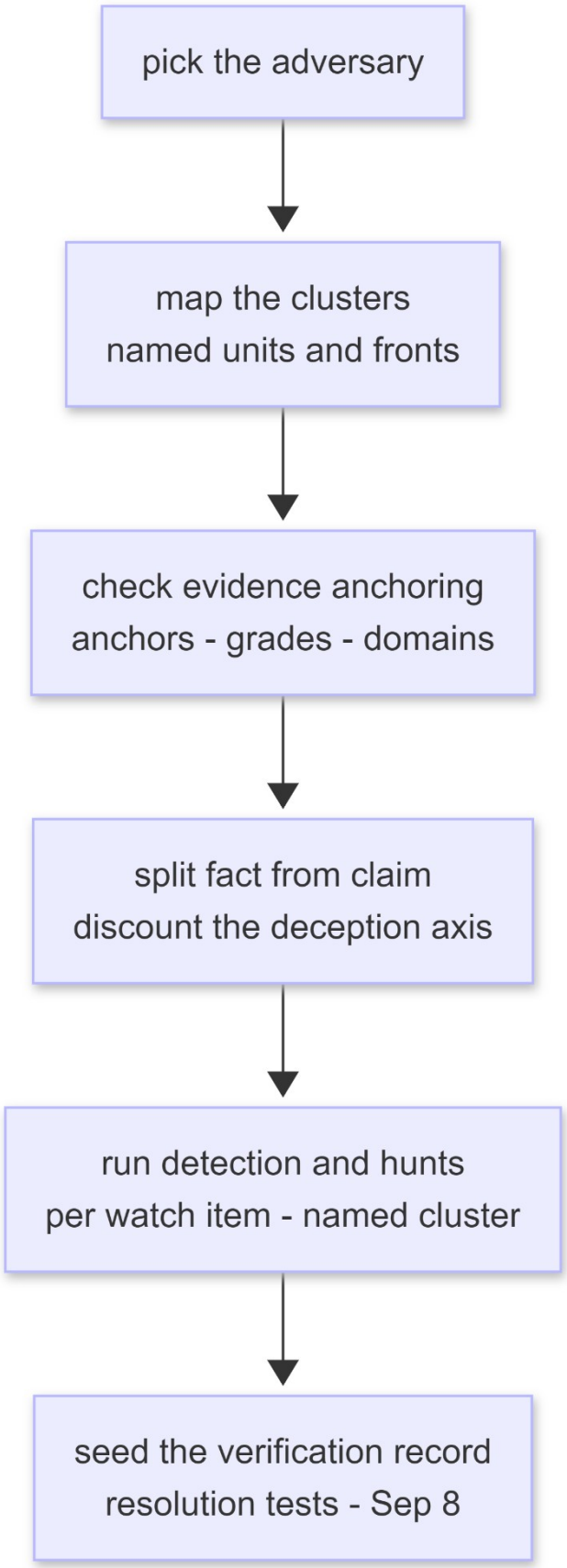


Figure F. Tactical Technical reader path

China — tactical

The Ministry of State Security and its contractors run APT41, APT31, APT40, and APT10; the People's Liberation Army runs military cyber under the 2024 reorganization. The positioning and espionage lines work through exploitation of known vulnerabilities in network edge devices — Ivanti, Citrix, Sophos, and Cisco IOS XE appliances among them — living-off-the-land persistence, valid-account and cloud abuse, and operational relay box networks that mask origin; one documented relay network spanned roughly 150 endpoints across 36 countries. The influence line works through inauthentic personas, AI-generated content, and platform-algorithm manipulation across five platforms. China carries 41 individually sourced anchors, 64 verified-fact indicators, and 18 at the top reliability rank — the richest open-source picture among the Big Four. Anchored domain averages read Military 5.50, Security 5.32, and Technical 5.50 on the 0–6 scale.

Anchor	Source basis	Grade
Volt Typhoon pre-positioning across communications, energy, transport, water	CISA, NSA, FBI joint advisory with Five Eyes	A2
Salt Typhoon backbone espionage across 80-plus countries	Joint advisory across 13 governments	B2
Activity confirmed live, February 2026	FBI; Norway and Singapore disclosures	B2
China-nexus intrusion up 38 percent in 2025; logistics up 85 percent	CrowdStrike 2026 Global Threat Report	B2
MSS contractor practices	i-SOON contractor leak, February 2024	B2

Verified effect stays split from adversary claim. Beijing's denials and counter-accusations read as adversary-originated and route to the deception axis. Carrier assertions that the Salt Typhoon intrusions stand contained read as unverified company assertion (ASA C3). 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 (IoC-2) as the earliest warning of the one observable.

The four China predictions enter the verification record at issue and resolve at the October 13, 2026 horizon. P1 resolves true if two independent vendor reports or one government advisory place initiating China-nexus access in the named target set; P4 resolves true if no confirmed China-nexus disruptive effect lands against a United States lifeline sector inside the horizon.

Russia — tactical

The GRU runs APT28 (Forest Blizzard), APT44 (Sandworm, Seashell Blizzard), Turla, and Storm-2372; the FSB runs Energetic Bear, Gamaredon, and the Center 16 and Center 18 structures; the SVR runs APT29 (Midnight Blizzard). Influence runs through Doppelganger and its RRN spoofed-outlet network, Storm-1516, Matryoshka, and Operation Overload. Disruption runs through NoName057(16), the DDoSia project, and the Cyber Army of Russia Reborn. The

lines work through edge-device exploitation, living-off-the-land persistence, token and OAuth abuse, and Telegram-tasked DDoSia infrastructure. Russia carries 35 individually sourced anchors. Domain-level anchored averages read Military 5.23, Security 5.00, and Technical 4.64 — concentration over breadth.

Anchor	Source basis	Grade
APT28 intrusion set tied to GRU Unit 26165	France ANSSI attribution, April 2025	Allied government, A-grade
Doppelganger influence infrastructure sanctioned	European Union sanctions on the Social Design Agency	A2
January denial-of-service campaign, ~160 domains, UK targets ~55 percent	SOCRadar	B2
GRU edge-device targeting of Western lifeline infrastructure	Amazon and Microsoft reporting	B2
Storm-1516 output more than doubled year over year	NewsGuard and Bloomberg	B2

Verified effect stays split from adversary claim. The influence content claims route to the deception axis; the intrusion and disruption lines carry vendor and government corroboration at B2. Hunt priorities: internet-facing appliance review against APT28 and APT44, living-off-the-land persistence against APT44 and APT29, token and OAuth abuse against APT29, Telegram tasking and DDoSia infrastructure against NoName057(16), and provenance and coordinated-inauthentic-behavior signals on suspected synthetic media. The access-to-effect transition (IoC-2) is the warning that moves the score toward the boundary.

North Korea — tactical

The Reconnaissance General Bureau directs the cyber program; the Lazarus Group and its TraderTraitor subset run the cryptocurrency thefts. The cryptocurrency line works through social engineering of insiders, bridge and multisig compromise, and a cross-chain laundering chain that holds proceeds before cashout. The IT-worker line works through stolen and fabricated identities, United States-based laptop farms, and front companies. The espionage line, including the Mach-O Man campaign, works through recruiter and investor impersonation and macOS-targeting malware.

Anchor	Source basis	Grade
$577 million in two April 2026 attacks (Drift, KelpDAO); 76 percent of 2026 crypto-hack losses	Blockchain-intelligence telemetry	B2
Bybit theft of about $1.46 billion in 2025, largest on record	FBI	A2
IT-worker scheme inside 100-plus firms; facilitator sentenced to nine years, April 2026	United States Department of Justice	A2

Anchor	Source basis	Grade
Cumulative attributed theft passes $6 billion since 2017	Blockchain-intelligence telemetry	B2
DPRK-Russia comprehensive strategic partnership, June 19, 2024	Government reporting	B2

The D-Score reads Operational — concealment over fabrication — so documented thefts carry at full grade and denials are discounted. The posture flag reads state-directed, the clearest case among the Big Four. Hunt priorities: custody and cryptographic-material controls, bridge and multisig governance, remote-hire identity and laptop-farm screening, unsolicited-outreach handling, and the move from theft to destructive effect (IoC-2) as the warning of the one observable. The forecast confidence reads Mature because on-chain telemetry instruments the revenue engine.

Iran — tactical

The IRGC Intelligence Organization and the IRGC Cyber-Electronic Command run one track; the Ministry of Intelligence and Security runs the other. Attributed clusters include APT35 (Charming Kitten, also Mint Sandstorm and Educated Manticore), APT42 the surveillance specialist, APT34 (OilRig), APT39, MuddyWater, and CyberAv3ngers. Tradecraft runs through in-memory backdoors, living-off-the-land persistence, trusted-cloud command-and-control, exposed industrial-control devices, and phishing.

Anchor	Source basis	Grade
CyberAv3ngers operations against exposed industrial-control systems	Joint government advisory; Treasury designation of six IRGC-CEC officials	A2
APT42 surveillance against dissidents and policy targets	Vendor reporting	B2
Cotton Sandstorm fast-reaction influence; AI-augmented personas	Platform takedown reporting	B2
Cyber tempo tracking the 2025–2026 kinetic confrontations	Open-source conflict reporting	B2
False attack claims and hacktivist fronts over state direction	Vendor and platform reporting	B2 (claims routed to deception axis)

The D-Score reads Elevated: Iran runs false attack claims, hacktivist fronts over state direction, and persona churn, so adversary-originated claims are discounted and carried apart. Hunt priorities: internet-exposed industrial-control inventory and segmentation, phishing and identity hardening against APT35 and MuddyWater, dissident-data protection against APT42, and false-claim verification during conflict windows. The kinetic-escalation wildcard and the tempo-decoupling falsifier (IoC-2) sit on the same watch line. Supreme Leader Ali Khamenei was assassinated in February 2026, and Iran's Assembly of Experts has since elected his son Mojtaba Khamenei, age 56, as the new Supreme Leader (corroborated by Iranian state media and multiple international outlets; ASA B2). The succession is resolved; the central wildcard is

now the consolidation of the new leadership and any factional fallout that reshapes the operator pipeline.

Field attribution — catalog-level read

The 38 actors below the Big Four carry attribution at catalog depth rather than the unit-level treatment the Big Four receive. The Iranian Axis attributes through Islamic Revolutionary Guard Corps Quds Force coordination, with Houthi anti-ship missile and drone activity and Hezbollah's standing military structure as the anchor evidence. The Salafi-jihadist cluster attributes through claimed-operation tempo and regional affiliate structure; intra-cluster scoring stays consistent because one analyst lane owns the full 12-actor band. The Russian-speaking ransomware ecosystem attributes through affiliate tradecraft and the state-tolerated, Commonwealth-of-Independent-States carve-out rather than to a single named crew.

Evidence discipline holds across the field. Verified facts separate from adversary claims at every tier. The Houthi movement's own ship-sinking and hit-rate tallies stay flagged and discounted; the verified Red Sea campaign tempo and the media operation carry the score. Hamas's October 2023 casualty and victory figures stay discounted; the verified command attrition and ceasefire-period tempo carry the read. Inflated hacktivist denial-of-service claims and jihadist propaganda tallies are marked and set aside, scored at the ASA grade the corroboration supports, generally B2 to B3.

The field carries the same resolution discipline as the Big Four. Each named one-observable doubles as a hunt and detection task. The Houthi reverses if Red Sea tempo narrows to Iranian-supplied systems without indigenous capability; Hamas reverses on reconstitution. An analyst converts each falsifier into a watch item and runs the test at the October 13 resolution, the same mechanical check the four states run.

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, and target-specific access detail holds for the Executive Desk band.

What the subscription editions add

This free edition scores the Big Four at depth across three tearlines and maps the full forty-two-actor field at catalog level. The subscription editions carry the field further and add the layers a working team, an enterprise, and a board each require.

The Analyst edition opens the seven actors below the Big Four to full sub-index depth and adds the analyst operating layer, collection and hunt priorities, an indicator tripwire register, quarter-over-quarter movers, a responsibility matrix, and a resourcing and readiness read. The Institutional edition opens all twenty-seven Tier 2 actors to STEMPLES Plus depth and adds the enterprise portfolio layer, cluster signatures, a sector-and-region exposure map, portfolio prioritization, and control-framework program mapping. The Executive Desk edition completes the field with the floor actors and the seven component annexes and adds the decision-

advantage layer, a composite weighted to the organization, active-probe collection under a mutual non-disclosure agreement, degradation-pathway tracking, scenario and wargame facilitation, and a named analyst with quarterly board briefings.

Each edition includes everything below it. Access by email to info@treadstone71.com.

Appendices

Appendix A — Acronyms and terms

Acronym or term	Full name	Function in the forecast
TAI	Treadstone 71 Adversary Index	Scores 42 named adversaries from 0 to 100 each quarter; the composite places the actor in a capability tier
Tier 0–Tier 3	TAI capability tiers	Tier 0 (80–100) peer-state; Tier 1 (55–79); Tier 2 (35–54); Tier 3 (0–34)
Boundary review zone	75–85 composite band	A composite inside the band sits under standing senior-analyst review at the tier line
CIQFM	Cyber Intelligence Quarterly Forecast Model	The forecasting engine behind the chapters
ASA	Adversary Scoring Architecture	The Treadstone 71 evidence and scoring system; its Evidence Standard expands the Admiralty Code into 30 factors
T / D / F-Score	Tri-score grades	Evidence quality, deception likelihood, forecast confidence
Sherman Kent terms	Words of estimative probability	Each term carries a defined band; Likely spans 55 to under 85 percent
ASA grade (e.g., B2)	ASA Evidence Standard grade	The classic letter–number anchor carried through the 30-factor screen
IoC	Indicator of change	A numbered tripwire; when it fires, the model revises the named judgment
COA	Course of action	Most Likely, Most Dangerous, and tail paths, each with an assigned probability
RGB	Reconnaissance General Bureau	North Korea's military intelligence directorate; runs the cyber program
MSS / PLA	Ministry of State Security; People's Liberation Army	China's civilian intelligence; the armed forces
GRU / FSB / SVR	Russian military, security,	Direct the Russian state

Acronym or term	Full name	Function in the forecast
	and foreign intelligence services	intrusion sets
IRGC / MOIS	Islamic Revolutionary Guard Corps; Ministry of Intelligence and Security	Direct the Iranian clusters
APT	Advanced persistent threat	A state-grade intrusion cluster tracked under a vendor designation
Operational technology	Industrial control systems	The systems running physical processes; written out in full throughout
Cultural Nexus	Seven-dimension terrain model	Scores the regime and population terrain from 0 to 100 per dimension; higher means tighter control
Frame A delta	Adaptation minus Institutional Rigidity	Reads forecast volatility; a deeper negative delta flags more surprise potential

Appendix B — Sources

Open-source reporting graded under the ASA Evidence Standard. The four chapters carry full numbered source lists in the working files; the consolidated set below names the load-bearing sources by actor. The Treadstone 71 internal baseline carries an A2 grade on the documented triangulation and peer-review record behind the catalog.

China: CISA, NSA, FBI Five Eyes Volt Typhoon advisory (A2); the 13-government Salt Typhoon advisory (A2); CrowdStrike 2026 Global Threat Report (B2); Spamouflage platform takedown reporting (B2); the i-SOON contractor leak (B2). Russia: France ANSSI APT28-to-GRU attribution (A-grade); European Union sanctions on the Social Design Agency (A2); SOCRadar DDoSia telemetry (B2); Amazon and Microsoft GRU edge-device reporting (B2); NewsGuard and Bloomberg Storm-1516 reporting (B2). North Korea: blockchain-intelligence telemetry on the 2026 thefts (B2); FBI on the Bybit theft (A2); United States Department of Justice on the IT-worker scheme (A2); the DPRK-Russia partnership of June 19, 2024 (B2). Iran: joint government advisory and the Treasury designation of six IRGC-CEC officials on CyberAv3ngers (A2); vendor reporting on APT42 surveillance (B2); platform takedown reporting on Cotton Sandstorm (B2); open-source conflict-tempo reporting (B2). Treadstone 71 TAI Q1 2026 baseline and ASA Evidence Standard baselines, internal (A2).

Actor or set	**Load-bearing sources**	**ASA grade band**
China	CISA-NSA-FBI Five Eyes Volt Typhoon advisory; 13-government Salt Typhoon advisory; FBI February 2026 disclosures; CrowdStrike 2026 Global Threat Report; i-SOON contractor leak	A2 to B2
Russia	France ANSSI APT28	A-grade to B2

Actor or set	Load-bearing sources	ASA grade band
	attribution (April 2025); EU sanctions on the Social Design Agency (Doppelganger); SOCRadar denial-of-service campaign data; Amazon and Microsoft GRU edge-targeting reporting; NewsGuard and Bloomberg on Storm-1516	
North Korea	FBI Bybit attribution; US DOJ IT-worker indictments and facilitator sentencing; blockchain-intelligence telemetry on 2026 theft value; government reporting on the DPRK-Russia partnership	A2 to B2
Iran	Joint government advisory and Treasury designations on IRGC-CEC and CyberAv3ngers; vendor reporting on APT42 surveillance; platform takedown reporting on Cotton Sandstorm; open-source conflict reporting on the kinetic cycle	A2 to B2
Field (38 actors)	Cluster inventories and the companion addendum one-pagers; regional government advisories; vendor and platform takedown reporting; academic forensic studies	B2 to B3
Treadstone 71 baseline	Documented three-source triangulation and peer-review record behind the catalog	A2 (internal)

The grade band reflects the strongest and the typical source per actor; individual anchors carry their own grade in the tactical tearline. Government and allied-attribution sources carry A-grades; most vendor reporting sits at B2. The field set runs lighter at B2 to B3, consistent with catalog-depth treatment. Full numbered source lists travel with the working files and the addendum.

Appendix C — ASA Evidence Standard (the standard in force)

Every judgment in the edition rests on evidence, and the ASA Evidence Standard grades how good that evidence is. The plain idea: a score means little unless the reader knows how solid the proof behind it is. So each finding carries a grade for the quality of its sources, a second grade

for how hard the adversary works to fool the analyst, and a third grade for how confident the forecast is.

Intelligence work has long graded sources with the NATO Admiralty Code — a letter for how reliable the source is (A through F) and a number for how credible the information is (1 through 6), so a grade of B2 reads usually reliable, probably true. That code dates to the 1940s and rates only the source and the claim. A modern adversary does more — generating fake video and fake personas, running coordinated fake-account networks, hiding state operations behind contractor cutouts or hacktivist fronts, and planning several moves ahead. The ASA Evidence Standard keeps the Admiralty grade as its starting point — the grade survives as two of the standard's 30 factors — and adds 28 more to reach what the old code does not: forensic chain of custody, whether a finding reproduces across separate vendors, synthetic-media risk, fake-network screening, active deception detection, and how the evidence fits the adversary's likely endgame.

The 30 factors group into nine clusters and produce three scores, the tri-score. The T-Score, from clusters C1 through C7, rates evidence quality. The D-Score, from C8, rates how much deception the picture carries, so the model discounts material that looks planted. The F-Score, from C9, rates forecast confidence. A grade such as B2 in the edition is the Admiralty starting read; the full screen behind it sets how much weight the finding actually earns.

Cluster	Weight (T-Score)	Factors
C1 Source Credibility	18%	F1 Source Reliability (Admiralty A–F anchor), F2 Authority, F3 Independence, F4 Access
C2 Information Validity	22%	F5 Corroboration, F6 Consistency, F7 Specificity, F8 Admiralty Credibility (1–6 anchor)
C3 Relevance	10%	F9 Topical Relevance, F10 Temporal Currency
C4 Cyber and Technical Integrity	15%	F11 Chain of Custody, F12 Technical Verifiability, F13 Metadata Integrity
C5 AI and Synthetic-Media Risk	12%	F14 AI-Generation Probability, F15 Provenance Adherence, F16 Manipulation Forensics
C6 Cognitive and Influence-Op Risk	13%	F17 Coordinated-Inauthentic-Behavior Indicators, F18 Propaganda and BEND
C7 Analytic Tradecraft Fit	10%	F19 Bias Disclosure, F20 Confidence Calibration
C8 Counterdeception (D-Score)	—	F21 Deception Density, F22 Cross-INT Discrepancy (weighted 28%), F23 Signature Anomaly, F24 Cover Story, F25 Action-Narrative Gap

Cluster	Weight (T-Score)	Factors
C9 Endgame Forecasting (F-Score)	—	F26 Target Convergence, F27 Capability-Intent, F28 Timeline Compression, F29 Cross-Domain Coordination, F30 Endgame Path

Classic anchor	Classic meaning	ASA treatment
A / 1	Completely reliable; confirmed	T-Score 90–100, Apex band
B / 2	Usually reliable; probably true	T-Score 70–89, Mature band; most vendor reporting sits here
C / 3	Fairly reliable; possibly true	T-Score 45–69, Operational band; single-source or partial corroboration
D / 4	Not usually reliable; doubtful	T-Score 20–44, Developing band; adversary-aligned or thin sourcing
E / 5	Unreliable; improbable	T-Score 0–19, Nascent band; deception channel or fabrication
F / 6	Reliability or truth cannot be judged	Routed to the D-Score; never scores on the T-axis alone

Appendix D — Control-framework cross-walk

The ranked defensive actions map to the control language a governance team already runs. The cross-walk below ties each action type to the NIST Cybersecurity Framework 2.0 functions and the CIS Controls v8 numbers, so a reader translates the forecast into the firm's own catalog without leaving the report. The mapping is a working reference; a control owner verifies each line against the firm's implementation.

Ranked action type	NIST CSF 2.0 (function · category)	CIS Controls v8
Edge-device and identity hardening; living-off-the-land hunts	Protect · PR.PS, PR.AA; Detect · DE.CM	4 Secure Configuration, 5 Account Management, 6 Access Control, 7 Continuous Vulnerability Management, 13 Network Monitoring
Communications protection; move sensitive traffic to end-to-end encryption	Protect · PR.DS (data in transit)	3 Data Protection, 12 Network Infrastructure Management
Intellectual-property segmentation and insider screening	Identify · ID.AM; Protect · PR.DS, PR.AA; Detect · DE.CM	3 Data Protection, 6 Access Control, 13 Network Monitoring, 14 Security Awareness
Custody, cryptographic-material, and multisig	Protect · PR.DS, PR.AA; Govern · GV.RM	3 Data Protection, 6 Access Control, 16 Application

Ranked action type	NIST CSF 2.0 (function · category)	CIS Controls v8
governance		Software Security
Denial-of-service resilience and rehearsed response	Protect · PR.IR; Respond · RS.MA; Recover · RC.RP	11 Data Recovery, 12 Network Infrastructure, 17 Incident Response Management
Segmented, tested backup and recovery	Recover · RC.RP; Protect · PR.DS	3 Data Protection, 11 Data Recovery
Operational-technology isolation and segmentation	Protect · PR.IR, PR.AA; Identify · ID.AM	12 Network Infrastructure, 13 Network Monitoring, 4 Secure Configuration
Supplier and managed-service review	Govern · GV.SC; Identify · ID.RA	15 Service Provider Management
Brand and narrative monitoring with pre-drafted response	Detect · DE.CM; Respond · RS.CO	13 Network Monitoring, 17 Incident Response Management

Produced under Treadstone 71 house analytic discipline against the CIQFM Model Architecture v1.9. Sherman Kent probability spectrum, ASA Evidence Standard tri-score with NATO Admiralty grading, base-rate anchoring, structured alternatives with falsifiers, and the verification record. Production disclosure per model Section 17: the analyst directed the forecast; an AI agent assisted drafting, figure production, and consistency verification, and the analyst approved each judgment and grade.