The Treadstone 71 Standard — What We Are Building, What It Solves, and Who Buys It

Document version: v1.2 — August 13, 2026 · Owner: Treadstone 71 — TAI Team · Purpose: A plain-language explanation of the Treadstone 71 Standard, the problem it solves, the value it delivers, and the customers it serves

The problem

Senior decision-makers cannot rank their adversaries on a common scale. The market offers them three types of products, but none of them finish the job.

Threat-intelligence vendors produce indicator feeds and threat-actor catalogs built for incident responders. The catalogs resist comparison across categories, so a reader cannot tell whether a nation-state cyber program outranks a ransomware crew or a state-backed influence network. Geopolitical houses produce regional narrative assessments that read well but lack a scoring board to act on. Specialist firms cover one slice each, cyber, terrorism, or influence operations, and silo the slices apart.

The senior consumer ends up doing the integration. A bank's chief information security officer, a government desk officer, a defense-prime risk lead, and a corporate board each stitch together cyber reporting, geopolitical context, and influence-operation analysis by hand, under time pressure, without a shared method. The integration work falls to the people least equipped to do it well, and the result is gut-level threat rankings dressed up as analysis.

The Treadstone 71 Standard moves the integration upstream, into the methodology, where it belongs.

What we are building

The Treadstone 71 Standard is a six-pillar body of work that scores, explains, and operationalizes adversary threat on a common, auditable scale. The pillars share one analytic spine: documented evidence, graded for quality, marked with Sherman Kent estimative language, and traceable from a headline score down to named open-source citations.

The first pillar carries the others. The remaining five extend the same method into tradecraft reference, public attribution, an open quality standard, a software platform, and a board-level advisory practice.

Pillar 1 — The Treadstone 71 Adversary Index (TAI)

The Adversary Index scores named adversaries across eight analytical dimensions on a single 0-to-100 composite scale, refreshed every quarter. The Q2 2026 catalog scores 42 actor profiles plus seven component annexes, spanning 73 points of operational range, from the most capable sovereign cyber power down through the remnants of a collapsed state. The inaugural quarterly release published July 15, 2026; the next release lands October 5, 2026, carrying the TAI Q3 refresh and the CWTR inaugural.

The Index solves the ranking problem directly. A reader compares a nation-state, a state-aligned proxy, a jihadist network, a cartel, a ransomware ecosystem, and a hacktivist crew on the same scale, because the method scores capability substance rather than threat-actor category. Two actors that reach the same composite through different strengths sit side by side, and the eight sub-indices show why. The score traces down through

the sub-indices, the indicator framework, and the cultural-context layer to the evidence underlying it, so a skeptical reader can audit the number rather than trust it.

The Index replaces qualitative adversary assessment with quantitative scoring that a customer can defend. Customers move from “we think China is the top threat” to a documented composite, a sub-index profile, a forecast horizon, and a citation trail.

The six pillars at a glance

Pillar	Name	What it solves
Pillar 1	TAI — Treadstone 71 Adversary Index	Ranks every adversary on one auditable 0-100 scale, refreshed quarterly, so decision-makers compare threats across categories rather than guessing.
Pillar 2	CWTR — Cognitive Warfare Tradecraft Reference	Documents the tradecraft behind influence and cognitive operations, so analysts recognize, name, and counter adversary maneuvers from a shared reference.
Pillar 3	PAS — Public Attribution Series	Publishes rigorous, evidence-graded attributions, so the market gains a trusted public record of who did what, separated from adversary claims
Pillar 4	DAS — open intelligence-quality standard	Defines what good intelligence evidence looks like and certifies against it, so the discipline gains a shared quality bar, the way other fields have audit standards
Pillar 5	CWOS — Cognitive Warfare Operating System	Delivers the method as software, so customers run the scoring, tracking, and analysis continuously rather than reading a quarterly report
Pillar 6	ECWO — board-level cognitive warfare retainer	Puts senior cognitive-warfare judgment on retainer in the boardroom, so executives and directors get standing advisory rather than one-off briefings.

The pillars reinforce each other. The Index (Pillar 1) supplies the scores. The Tradecraft Reference (Pillar 2) explains the adversary behavior behind the scores. The Public Attribution Series (Pillar 3) demonstrates the method openly. The quality standard (Pillar 4) certifies the evidence discipline. The Operating System (Pillar 5) runs the whole method continuously. The board retainer (Pillar 6) carries the judgment into the rooms where decisions get made.

The so what

Three things change for the customer.

First, threat ranking becomes defensible. A risk owner who allocates a defensive budget, a desk officer who briefs a principal, and a director who sets enterprise risk appetite each point to a documented score with a citation trail rather than to professional intuition. The number survives scrutiny because the method shows its work.

Second, integration stops being the customer's burden. The Standard scores cyber, cognitive, and kinetic capability in a single model, so the senior consumer reads an integrated result rather than assembling one under a deadline.

Third, change becomes visible. The quarterly cadence and trajectory tracking show which adversaries gain capability, which degrade, and through which pathway. A snapshot tells a customer where an adversary stands today. The Standard tells them where the adversary is heading, with the confidence marked in estimative language.

Who buys

The Adversary Index reaches customers through four subscription tiers that map catalog coverage and analytical depth to the buyer's role.

Tier	Annual price	What the buyer gets	Who buys
Tier 0	Free	Methodology framework, the Big Four composite scores, and the two sovereign-power standalone profiles	Prospects evaluating the offering, academic researchers, journalists, and university courses
Tier 1 — Analyst	$25,000	Tier 0 plus the 7 Tier 1 actors at full sub-index depth (11 adversaries scored)	Individual analysts, university research centers, smaller security firms, and mid-sized financial institutions
Tier 2 — Institutional	$75,000	Tier 1 plus the 27 Tier 2 actors with full indicator detail (38 adversaries scored)	Major banks, Fortune 500 corporate security teams, defense contractors, government intelligence units, and threat-intelligence vendors
Tier 3 — Executive Desk	$250,000	Tier 2, plus the Tier 3 actors, the component annexes, and direct analyst access	Senior government executives, top-tier financial institutions, major defense primes, national infrastructure operators, intelligence agency partners, and corporate boards

The free tier earns credibility through public scrutiny and seeds adoption among researchers and journalists. Most paying customers start at the Analyst tier and move to the Institutional tier as their coverage needs grow. The Executive Desk tier serves the organizations that need the full catalog, the component annexes, and a named analyst on call.

The latter pillars widen the buyer base. The Tradecraft Reference and the Public Attribution Series reach the analytic and academic communities, as well as the press. The open quality standard applies to the discipline as a whole, including vendors and government units that adopt it as a certification bar. The Operating System reaches customers who want the method to run continuously in their own environment. The board retainer reaches the executives and directors who bear the ultimate risk.

In one sentence

The Treadstone 71 Standard turns adversary threat from a matter of expert intuition into a documented, auditable, quarterly-refreshed score that any decision-maker can compare, defend, and act on. The six pillars

carry that method from a published index through tradecraft reference, public attribution, an open quality standard, a software platform, and a board-level advisory practice.

Document control

Field	Value
Document title	The Treadstone 71 Standard — What We Are Building, What It Solves, and Who Buys It
Version	v1.2 — August 13, 2026 (supersedes v1.1 of June 30, 2026)
v1.2 change note	Reconciles the inaugural release date to July 15, 2026 and records the October 5, 2026 release (TAI Q3 refresh plus CWTR inaugural). No content change beyond dates.
Owner	Treadstone 71 — TAI Team
Companion documents	TAI Q2 2026 Tier 0 Edition; TAI methodology white paper; subscription tier sheet