TREADSTONE 71

Strategic Cyber Intelligence · Clandestine HUMINT · Cognitive Warfare

Capability Statement

May 2026 · Edition 2026.2

Treadstone 71 is a woman- and veteran-owned small business exclusively focused on cyber and threat intelligence consulting, services, training, and counterintelligence. We are a pure-play intelligence shop. Intelligence is our only business.

Since 2002, we have built adversary dossiers, infiltrated hostile online ecosystems, advised boards and senior government leaders, and trained the analysts and operators who run intelligence functions at banks, defense agencies, NATO, allied military intelligence services, and Fortune 500 enterprises across four continents.

We See What Others Cannot.

Organizations bring Treadstone 71 in when the facts do not line up — when threat reporting feels thin, when leadership needs more than technical jargon, or when a fast-moving event demands verified intelligence instead of guesswork.

Clients call when they need answers to questions such as:

- Who sits behind the threat?
- What does the adversary want?
- Which narratives shape the operation?
- Where do the real pressure points sit?
- Which warning signs matter now?
- What should leadership do next?

Treadstone 71 answers those questions with intelligence discipline, field-tested judgment, and clear reporting built for action.

Company Identifier Block

Treadstone 71 LLC is registered for federal, state, commercial, and allied government contracting. Identifiers and points of contact are listed below.

Legal Name	Treadstone 71 LLC
Status	Woman- and Veteran-Owned Small Business (WOSB / VOSB)
UEI / DUNS	DUNS 109967419
NAICS Codes	541519, 541611, 541618, 541690, 611420
Headquarters	13530 Sabal Pointe Dr, Fort Myers, FL 33905
Phone / Fax	331.999.0071 (office) · 508.519.0363 (fax)
Primary Email	info@treadstone71.com
Point of Contact	Jeffrey S. Bardin, Chief Intelligence Officer · 207.415.4021 · jbardin@treadstone71.com
Established	2002 (intelligence consulting) | 2009 (formal training)
Tagline	We See What Others Cannot.

Digital Properties

Property	Function
www.treadstone71.com	Corporate site — services, intelligence offerings, advisory
www.cyberinteltrainingcenter.com	Training platform — certifications, stacks, on-demand courses
www.cybershafarat.com	Online blogging site
Treadstone 71 on YouTube / Substack	Open intelligence dissemination, briefings, commentary

Operational Pedigree and Authority

The capability to operate within hostile information ecosystems is not built solely through network engineering. It is forged in military intelligence, regional immersion, and decades of high-stakes tradecraft. Treadstone 71's leadership pedigree gives the firm a posture no commercial-only competitor can replicate.

Foundational Disciplines

Foundational Discipline	Institutional Origin	Strategic Intelligence Application
Cryptologic Linguistics	United States Air Force	Interception, translation, cryptanalysis, and psychological analysis of adversary communications; dialectical mastery.

Foundational Discipline	Institutional Origin	Strategic Intelligence Application
Tactical Reconnaissance	U.S. Army / Army National Guard (armored scout platoon leader, 2Lt)	Kinetic scouting principles — OPSEC, terrain analysis, route evaluation — translated to digital infiltration.
Socio-Cultural Fluency	Trinity College (BA, Middle East Studies & Arabic); Colgate (Russian); Middlebury (Advanced Arabic); in-country Jeddah, KSA 1988–1989	Deep comprehension of Middle Eastern and Russian geopolitical histories, fueling persona authenticity and adversary modeling.
Information Assurance	Norwich University (M.S. in Information Assurance)	Enterprise risk framing, cryptography, systemic risk management, and executive-grade advisory.
Operational Codification	Treadstone 71 (founded 2002); adjunct faculty at Utica College and Clark University	Field-tested CIA/DIA-style tradecraft formalized into master 's-level cyber intelligence curricula.

The Masterpiece Operation — Zabihullah Mujahid

Founded in 2002 to address the intelligence gap created by terrorist use of the early internet, Treadstone 71 shifted from passive observation to active, clandestine engagement by 2004. The firm systematically built deep-cover cyber personas inside password-protected Al-Qaeda websites, dark-web forums, and encrypted chat channels. Raw intelligence from those infiltrations — tactical attack planning, location analysis, hidden funding streams — was disseminated to U.S. defense, law enforcement, and intelligence organizations, in many cases providing IP addresses of newly established extremist infrastructure before the sites had fully propagated.

Between approximately 2010 and 2012, Treadstone 71 successfully impersonated the Taliban spokesperson alias "Zabihullah Mujahid" across forums, social media, and electronic media, including international news organizations such as Al Jazeera. Maintaining the persona required absolute linguistic perfection across Arabic, Pashto, and Urdu colloquialisms; flawless ideological consistency with Salafi-jihadist theological frameworks; a multi-layer anonymization architecture (nested VPNs, rotating proxy chains, air-gapped persona hardware); and the willingness to engage in calculated tactical sacrifice, active sabotage of adversary communications, and psychological provocation to build credibility inside paranoid networks.

After roughly sixteen months of building the persona, Treadstone 71 executed a calculated slow-burn teardown — fabricating a defection narrative, then systematically dismantling Taliban propaganda from inside the network and exposing the organization's hypocrisy on drug smuggling and inflated ISAF combat claims. The full operational history, including target exploitation methodology and the never-shared CyberIntellipedia knowledge base, is documented in the Treadstone 71 Operational Dossier (T71 Pedigree).

Why This History Matters Today

The same disciplines that sustained "Zabihullah Mujahid" across two years of adversary scrutiny now power Treadstone 71's commercial and government work: persona OPSEC, adversary cognitive modeling, cultural and linguistic source evaluation, deception planning, and the codified analytic doctrine taught at master's level at Utica College and Clark University.

> Clients do not hire a vendor. They hire a discipline.

What Clients Hire Treadstone 71 To Do

Engagements span board-level advisory through hands-on adversary infiltration. The table below summarizes the present-day service categories and the value each delivers.

Service	What Clients Gain
Adversary Targeting	Adversary profiles, network ties, motive, centers of gravity, and attack indicators.
Strategic Warning Intelligence	Early signals before noise becomes a crisis; forecasts and estimates as intelligence intends.
Cyber HUMINT	Insight from hostile online communities, deceptive personas, and covert influence activity.
Cognitive & Influence Operations	Discovery, attribution, and counter-measurement against disinformation, narrative weaponization, and cognitive warfare.
AI-Augmented Intelligence	Decision Advantage engines, generative-AI analytic acceleration, and Sovereign AI audit and governance.
Executive Advisory	Board-ready threat translation, risk framing, and decision support — including Interim Head of Intelligence engagements.
Intelligence Training	Analysts who judge sources well, write clearly, and brief leaders under pressure — across 48+ courses and four certification tiers.
Investigations & Crisis Support	Fast triage, verified reporting, stakeholder mapping, and sharper situational awareness during fast-moving events.

Core Capability Areas

Cyber Intelligence — Consulting and Services

All services are contextually tailored to client intelligence requirements. We do not run a create-once-deliver-many model.

- Adversarial Baseball Cards and adversary dossier development
- All-Source Intelligence Operations
- Analysis as a Service — reports, briefs, and dossiers
- Conspiracy Theories analysis and weaponization detection
- CounterIntelligence Research and Analysis
- Cyber and Threat Intelligence Program Build (engagement and 12-month online)
- Cyber Counterintelligence in Cryptocurrency Investigations
- Cyber Intelligence Capability Maturity Model (CMM) Assessment
- Cyber Operations — Influence Operations and Analysis
- Disinformation, Misinformation, and Malinformation Detection, Analysis, and Counter Operations
- Generative AI Cyber Intelligence and Counterintelligence

- Influence Operations / Cognitive Warfare Assessment, Discovery, and Counter Operations
- Interim Head of Intelligence (executive embed)
- Internal Intelligence Communities of Interest design and build
- Intelligence Requirements Development (PIRs / EEIs)
- Mastering Cybercrime Intelligence — advanced strategies
- OPSEC Assessment and Intelligence Preparation of the Cyber Battlefield (IPCB)
- STEMPLES Plus geopolitical/strategic research
- Strategic Intelligence Services
- Targeted Research — client-driven
- Threat Intelligence Assessments
- Workshops for Intelligence Teams

New and Expanded Offerings

Six high-leverage advisory and assessment products added since 2025, designed for boards, CISOs, general counsel, and high-risk enterprises.

- **Intelligence Readiness Score —** a 15-question diagnostic across five intelligence domains producing a quantified readiness score, industry benchmark comparison, and a board-ready report. Available as a self-service assessment at treadstone71.com.
- **Adversary Exposure Briefing —** a fixed-scope, time-bounded engagement that delivers a verified picture of who is interested in the client, what they want, which channels they exploit, and where decision-makers should focus.
- **Cognitive Warfare Readiness Drill —** a tabletop and live-fire exercise modeling adversary narrative attacks, reflexive control attempts, and influence-operation kill chains against the client's executive and communications functions.
- **Monthly Intelligence Dispatch —** a recurring subscription product delivering vetted, sector-aware intelligence on adversary movement, narrative trajectory, and emerging threats — written for executive consumption.
- **Sovereign AI Audit —** paid governance and risk audit of enterprise AI deployments, covering adversarial robustness, prompt-injection exposure, model supply chain, data sovereignty, and intelligence integration.
- **Quiet Vetting —** discreet personnel and counterparty vetting service — OSINT and persona-level due diligence for high-trust hires, partners, and acquisitions, executed without alerting the subject.

Decision Advantage — AI-Infused Intelligence Engines

Treadstone 71's Decision Advantage capability stack pairs human intelligence tradecraft with purpose-built AI engines. Each engine is operated as a managed advisory service or an embedded enterprise capability.

Engine	Full Name	Function
ATCRI	**Adversary Targeting & Cyber Risk Intelligence**	Continuous adversary dossiering — capability, intent, infrastructure, and attack indicators — fused with enterprise risk framing.
ACS	**Adversary Cognitive Signals**	Real-time signal extraction from adversary information ecosystems; narrative trajectory and intent forecasting.

Engine	Full Name	Function
CWC	**Cognitive Warfare Countermeasures**	Detection, attribution, and response to influence operations, narrative weaponization, and reflexive control.
CWIA	**Cognitive Warfare Impact Assessment**	Quantified measurement of cognitive-attack effect on stakeholder populations, decision cycles, and operational tempo.
HTIM	**Hostile Threat & Insider Mapping**	Insider risk modeling fused with external adversary mapping, behavioral indicators, persona-OPSEC, and quiet Vetting.
CARM	**Cyber Adversary Reasoning Model**	Adversary decision-modeling and red-team reasoning engine — anticipates adversary choices under uncertainty.

Generative AI Augmentation

Integration of generative AI extends Treadstone 71's intelligence delivery across four directions:

- **AI-Driven Threat Intelligence Analysis** — automated adversarial profiling beyond static baseball cards, with profiles that evolve against real-time signal feeds; predictive intelligence drawing patterns from historical data to surface preemptive warning.
- **AI for Influence Operations** — automated disinformation detection with impact and counter-measure reporting; counter-narrative generation tailored to channel, audience, and adversary.
- **AI-Powered Training and Simulation** — scenario-driven cyber-defense exercises and adaptive learning pathways calibrated to each analyst's progression.
- **Cognitive Warfare AI** — deepfake detection, memetic-warfare strategy generation, and adaptive cognitive-bias identification for both analysts and adversaries.
- **AI-Enhanced CyberIntellipedia** — real-time intelligence dashboard layered over Treadstone 71's curated knowledge base.

Clandestine Cyber HUMINT

Engagements that require non-attributable presence inside adversary ecosystems — forums, encrypted channels, social platforms, dark-web marketplaces — are executed against the same operational doctrine that sustained the Zabihullah Mujahid operation. Capabilities include persona engineering and aging, multi-layered anonymization architecture, target-language fluency and dialectical mastery, deception planning, source validity scoring, and structured analytic handoff to client decision-makers. All work is lawful, ethical, and client-authorized; engagements are scoped under written terms.

Influence Operations and Cognitive Warfare

Discovery, attribution, measurement, and countermeasure design against adversary cognitive operations. Engagements range from one-time narrative-trajectory assessments to long-term measurement of nation-state influence campaigns. The methodology integrates STEMPLES Plus, Cialdini's principles, the Seven Radicals, the Dark Triad/Pitch-Black Tetrad, Hofstede dimensions, and the Iranian and Russian cognitive warfare doctrines published in Treadstone 71 research.

Training Portfolio

Treadstone 71 training has been delivered since 2009 under intelligence-community standards adapted to the cyber threat environment. The current platform — cyberinteltrainingcenter.com — hosts a structured catalog of 48 production courses organized into four tiers.

Tier / Band	Catalog Coverage
Tier 1 — Core Certifications	Flagship CCIA, CCCI, CCIA In-Person, CCCI In-Person, Crypto-CCCI, Strategic Intelligence, Cyber Threat Intelligence Program Build, Transnational Cybercrime, PEOPINT, Intel/Counterintel Bundle, Master Tradecraft Bundle.
Tier 1.5 — Career Stacks	Analyst Stack ($6,999 · 10 courses · ~80 hr · 31% savings) · CounterIntelligence Stack ($3,999 · 11 courses · ~100 hr · 37% savings) · AI-Infused Cognitive Stack ($6,999 · 13 courses · ~120 hr · 16% savings) · Master Tradecraft Bundle ($6,999 · 46% savings vs. $13,000 strike) · Enterprise Subscription ($99,990/yr).
Tier 2 — Cognitive Warfare & Regional	Cognitive Warfare Definitions, NATO PsyOps, Russian Cognitive Warfare (Parts 1 & 2), Russian Stemples, Russian APT, Chinese Cognitive Warfare, Iranian Cognitive Warfare, Iranian Stemples, Disinformation, Color Revolutions, Conspiracy Theories, Dark Triad / Pitch-Black Tetrad, Seven Radicals, Big Five (OCEAN), Myers-Briggs Under Pressure, Cialdini's Principles, Cyber CointelPro.
Tier 3 — Methodology Specialists	Structured Analytic Techniques ($1,499 flagship), Analytic Writing ($899), Critical Thinking ($899), STEMPLES Plus ($399), Stakeholder Analysis ($399), Collection Management ($399), Source Evaluation ($399), Intelligence Requirements ($299), Insider Threats ($999), Persona OPSEC ($499), Adversary Targeting ($299), Deception Planning ($199), Dirty Tricks ($99), Cyber Warfare ($1,999 AI Cog Stack flagship).

Master Certifications and Flagship Programs

- **Certified Cyber Intelligence Analyst (CCIA)** — the flagship cyber intelligence tradecraft certification, taught online and in-person.
- **Certified Cyber Counterintelligence Analyst (CCCI)** — counterintelligence, influence operations, denial and deception, online and in-person.
- **Crypto-CCCI** — counterintelligence specialization for cryptocurrency investigations and adversary financial tracking.
- **Master Tradecraft Bundle** — combined CCIA + CCCI + methodology specialists at $6,999 (46% savings vs. $13,000 strike price).

Career Stacks (Tier 1.5)

- **Analyst Stack** — $6,999 · 10 courses · ~80 hours · 31% savings. End-to-end analyst tradecraft from collection to dissemination.
- **CounterIntelligence Stack** — $3,999 · 11 courses · ~100 hours · 37% savings. Full counterintelligence and influence operations track.
- **AI-Infused Cognitive Stack** — $6,999 · 13 courses · ~120 hours · 16% savings. Cognitive warfare and AI-augmented intelligence.
- **Enterprise Subscription** — $99,990/year. Organization-wide access for intelligence teams.

Tier 2 — Cognitive Warfare and Regional Catalogs

Eighteen courses covering NATO PsyOps, Russian and Chinese cognitive warfare, Iranian information operations, color revolutions, disinformation, conspiracy theory weaponization, and the psychological frameworks (Dark Triad, Seven Radicals, Big Five / OCEAN, Myers-Briggs under pressure, Cialdini's principles, Hofstede dimensions) used in adversary modeling.

Tier 3 — Methodology Specialists

Fourteen short-format courses for analysts who need to drill on a specific tradecraft skill — Structured Analytic Techniques (flagship at $1,499), Analytic Writing, Critical Thinking, STEMPLES Plus, Stakeholder Analysis, Collection Management, Source Evaluation, Intelligence Requirements, Insider Threats, Persona OPSEC, Adversary Targeting, Deception Planning, Dirty Tricks, and Cyber Warfare (AI Cog Stack flagship at $1,999).

Delivery Modes

- On-demand online (cyberinteltrainingcenter.com)
- Instructor-led virtual (private cohort)
- In-person and on-site (CCIA In-Person, CCCI In-Person, custom)
- Customized and private engagements
- Subscription training service for ongoing organizational uplift
- Bundles — Joint Tradecraft Topics; Cyber Intelligence and Counterintelligence — Jihadist Topics; Targeted Adversaries — the Middle East

Recognition, Authority, and Trust Markers

Recognition / Authority	Present-Day Value
RSA Conference — Excellence in the Field of Security Practices (2007)	Validated intelligence-driven approach to enterprise security at the highest industry level.
SC Magazine — Best Security Team (2007)	Operational discipline for investigations, incident response, and high-trust security work.
NATO Cooperative Cyber Defence Centre of Excellence (CyCon)	Keynotes and classified briefings on cyber intelligence, cognitive warfare, and infiltration methodology.
U.S. Naval Academy / Air Force Institute of Technology	Senior-leader education and doctrine support for hard missions.
Boston InfraGard — Board Leadership	FBI/private-sector infrastructure protection; OSINT instruction to FBI special agents.
Cloud Security Alliance — Founding Member	Early architect of cloud security governance frameworks.
Boards & Editorial	Potomac Institute for Policy Studies, Journal of Law and Cyber Warfare, Content Raven, Wisegate.
Faculty	Utica College and Clark University — first formal academic codification of CIA/DIA-style tradecraft for the cyber domain.

Recognition / Authority	Present-Day Value
Media Authority	CNN, CBS News Live, Fox News, BBC Radio, BBN, i24News, Business Insider — primary, trusted authority on cyber crime, cyber terrorism, and strategic intelligence.

Past Performance — Training and Services

Engagements span four continents and include defense, intelligence, financial services, healthcare, energy, technology, and federal civilian sectors. Several organizations are not listed due to contract or classification requirements.

Defense, Intelligence, and Government

NATO, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), U.S. Department of Defense, U.S. Naval Academy, Air Force Institute of Technology, FBI (Boston InfraGard / OSINT instruction), Naval Air Warfare Center, NASA, National Reconnaissance Office, Defense Security Services, Belgian Military Intelligence, Singapore Ministry of Defence, Dutch Police, NCSC NL, Finance CERT Norway, Bank of Canada, Egyptian Government, Malaysian Cyberjaya, Abu Dhabi Smart Solutions and Services Authority, Expo2020, State of Florida.

Financial Services

American Express, Capital One, Bank of America, Bank of America Merrill Lynch, JP Morgan Chase, Goldman Sachs, Citi / Citigroup, Wells Fargo, PNC, U.S. Bank, T. Rowe Price, Fidelity Investments, Schwab, TD Ameritrade, Discover, Equifax, BB&T, KeyBank, Northern Trust, Fannie Mae, Synchrony Financial, MetLife, New York Life, Mass Mutual, BNY Mellon, UBS Group, Credit Suisse, HSBC, Barclays, Santander, BBVA, ING, DNB Norway, Euroclear, Bridgewater Associates, Vista Equity Partners, Tower Research, Geller & Company, Baupost Group, Commonwealth Bank, Standard Chartered, OCBC Bank Singapore, Mitsubishi UFG Trust and Banking, Nomura International, ANZ, National Australia Bank, Raymond James, Vantiv, Verizon, OCC (Options Clearing Corporation), Intercontinental Exchange (ICE), Nacha, ACI Universal Payments, Promontory Interfinancial Network, Betaalvereniging Nederland, M&T Bank, First Citizens Bank, Citizens Financial Group, Regions Financial, Huntington, Western & Southern, Essent, Black Knight Financial, Tri Counties Bank, Bank of North Carolina, Ocean First Bank, American National Bank of TX, Farm Credit Services of America, PenFED, People's United Bank, East West Bank, Thrift Savings Plan, Wyndham Capital, Scottrade, iPipeline, Aviation ISAC.

Technology, Defense Industrial Base, and Critical Infrastructure

Lockheed Martin, General Electric, General Motors, Sony, Dell Secureworks, HPE Security, Symantec, Palo Alto Networks, Intel Corporation, Salesforce, Motorola Solutions, EclecticIQ, Anomali, SITE SA, Stellar Solutions, DarkMatter (UAE), PNY, Battelle, Columbus Collaboratory, Content Raven, American Electric Power, Nationwide, Cardinal Health, L Brands, Home Depot, Target, Archer Daniels Midland, Merck & Co., W.R. Berkley.

Healthcare, Legal, Insurance, and Professional Services

Cleveland Clinic, OhioHealth, Harvard Pilgrim, Blue Cross Blue Shield Michigan, Aetna, QBE Insurance Group, Deloitte, Ernst and Young, Latham and Watkins LLP, Church of Jesus Christ of Latter-Day Saints, PayPal, VISA, plus additional firms by proxy through analysts trained at Treadstone 71.

Intellectual Property and Authority

Multiple registered copyrights covering course content, methodologies, and reference guides.

Trademark in process for Treadstone 71.

Foundational publications include: The Illusion of Due Diligence — Notes from the CISO Underground; Current and Emerging Trends in Cyber Operations; multiple editions of the Computer Information Security Handbook; and additional volumes on Islamic history and theological foundations supporting cultural intelligence work.

Media authority: CNN, CBS News Live, Fox News, BBC Radio, BBN, i24News, Business Insider.

Differentiators

- **Pure-play intelligence shop.** Intelligence is our only business — not a side capability bolted onto a managed-services or red-team practice.
- **Operational provenance.** Tradecraft taught and delivered at Treadstone 71 is field-tested in the most demanding clandestine environments — not derived from textbooks.
- **Cultural and linguistic depth.** Arabic, Russian, and regional fluency; in-country experience; and decades of adversary-culture modeling.
- **Codified doctrine.** Methodologies formalized through master 's-level curricula at Utica College and Clark University, and a 48-course public training catalog.
- **AI-augmented, human-led.** The Decision Advantage engine stack pairs generative AI with intelligence judgment — neither replaces the other.
- **Contextual products, not commodity reports.** Every deliverable is tied to the client's intelligence requirements. We do not create once and deliver many.
- **Lawful, ethical, client-authorized.** Every engagement supports lawful, ethical, client-authorized work in defense, security, investigations, and resilience.

Engage Treadstone 71

Request a private briefing. Schedule an intelligence assessment. Engage Treadstone 71 for adversary targeting, cognitive warfare countermeasures, intelligence program build, or executive advisory.

Primary Point of Contact

Jeffrey S. Bardin · Chief Intelligence Officer

Treadstone 71 LLC

13530 Sabal Pointe Dr · Fort Myers, FL 33905

Office: 424-234-3629 · Direct: 207.415.4021

jbardin@treadstone71.com · info@treadstone71.com

www.treadstone71.com · www.cyberinteltrainingcenter.com

We See What Others Cannot.