The Cognitive Warfare Tradecraft Reference

Tier 0 Free Edition

Pillar 3 of the T71 Standard · Treadstone 71

Version 1.0 · Release date October 5, 2026

Nine families · 62 maneuvers · the method in full · one complete entry

© 2026 Treadstone 71 · Free to share and cite with attribution

Bottom Line

Intrusion tradecraft earned a shared language more than a decade ago. A defender names a technique, cites its identifier, and trusts a colleague in another country to mean the same thing. Cognitive warfare never got that. Analysts still describe one state influence maneuver under a dozen vendor names. A policymaker reading two reports has no way to tell one operation from two.

The Reference fixes the vocabulary. Sixty-two maneuvers get names across nine families. Each carries a permanent identifier and a two-sentence definition that states its boundary. Beneath them, 107 techniques record how each maneuver gets carried into practice. Every full entry rests on dated, graded evidence, keeps adversary claims apart from the verified record, maps to the DISARM framework, and names the observation that proves it wrong.

The free edition publishes the whole taxonomy and the whole method. Argue with the names and definitions in public. That is the point. The graded evidence, the technique layer, detection signatures, and countermeasures sit in the paid tiers.

What the Reference Is

The Reference is a versioned compendium. Not a feed. Version 1.0 holds three layers.

Layer	Count	What it records
Family	9	The strategic purpose shared by a group of maneuvers
Maneuver	62	A named, repeatable pattern of cognitive attack, with doctrine, indicators, exemplars, and a falsifier
Technique	107	The concrete implementation beneath a maneuver, with detection signatures and countermeasures

Table 1. The three layers of version 1.0.

Two annexes travel with the Institutional and Executive Desk tiers. The first registers how adversaries now build influence operations with AI, from doctrine files to paid amplification. The second crosswalks every entry to DISARM.

A quarterly Cognitive Warfare Tradecraft Report carries every change between editions: new entries, revised entries with rationale, shifts in actor tempo, a case of the quarter, and a public account of which falsifiers fired. The first report publishes with the free edition, and its public summary goes to every reader.

How to Read the Taxonomy

Every maneuver carries a permanent identifier, CW-M0001 upward. Numbers never get reused. Family assignment lives as metadata, not inside the number, so a maneuver that moves families keeps its identifier and the serials within a family run out of order by design.

Each maneuver names its primary doctrinal anchor: CN for Chinese doctrine, RU for Russian, IR for Iranian, DPRK for North Korean, and Gen for a pattern many actors share. The anchor marks where the lineage research starts. Other actors run the same maneuver, and full entries name them.

Four maneuvers carry a provisional mark. Each rests on one graded exemplar. One is not enough. The publish rule demands two for a full entry, so these four publish as Provisional until a second case lands, scheduled for the January 15, 2027 Tradecraft Report.

The Method

The entry schema

A full maneuver entry runs fifteen fields in fixed order.

#	Field	What it holds
1	Identifier	Permanent serial, never reused
2	Name	Verb-noun form in plain language
3	Aliases	Vendor, academic, and adversary names for the same pattern
4	Definition	Two sentences at most, with the boundary stated
5	Family	Metadata assignment, movable with logged rationale
6	Doctrinal lineage	Origin doctrine with dated sources, adversary primary text first
7	Observable indicators	Ranked by specificity
8	Exemplar cases	Two or three dated cases, each graded
9	Actor instantiation	Actors observed running the maneuver, linked to their Treadstone 71 Adversary Index scores
10	Adversary claims	Self-attributed reach or effect, kept apart from the record
11	Detection signatures	Observables a collector or platform measures

#	Field	What it holds
12	Countermeasures	Paired counters with graded feasibility
13	Falsifier	The observation that breaks the entry or its attribution
14	DISARM crosswalk	A mapped identifier, or a logged finding that none exists
15	Change log	Version, date, editor, and rationale for every revision

Table 2. The fifteen-field maneuver schema.

Techniques run a lighter eight-field schema beneath their parent: definition, implementation, observable signature, exemplar case, actor use, detection signature, countermeasure, and DISARM crosswalk.

Evidence discipline

A maneuver without two graded cases publishes only as Provisional, and the entry says so. The rule holds even where doctrine spells out the behavior, because the Reference documents conduct. Theory stays out.

Every exemplar carries a grade under the ASA Evidence Standard, first published in September 2026 (all versions: DOI 10.5281/zenodo.22662241). The standard scores evidence on 30 factors in nine clusters and reports three numbers: a T-Score for evidence quality, a D-Score for the probability that an adversary shaped the evidence, and an F-Score for confidence in the most likely achieved endgame. Source reliability and information credibility appear as a letter and a digit, the lineage of the NATO Admiralty code, and the two axes never get averaged.

Adversary claims never share a sentence with verified fact. A persona that claims a breach, a ministry that denies an atrocity, a vendor that markets an offensive platform as defense: each claim sits in its own sentence, marked as a claim.

Probability language

Forward judgments use fixed words tied to fixed ranges.

Term	Probability range (percent)
Almost certain	95 to 99
Highly likely	85 to <95
Likely	55 to <85
Roughly even chance	45 to <55
Unlikely	15 to <45
Highly unlikely	5 to <15
Almost no chance	1 to <5

Table 3. Estimative language used across the Reference.

DISARM: map, never clone

DISARM already catalogs disinformation techniques. The Reference maps to it. Copying stays off the table. Every entry carries a crosswalk row or a logged finding that no DISARM node fits. The crosswalk is Treadstone 71's own mapping; the fit of each row reflects analyst judgment, and no outside reviewer has confirmed it for version 1.0. Version 1.0 checked all 321 crosswalk rows against the current DISARM master data before release. Where no node fits, the gap goes to a public backlog for the framework's maintainers. The Reference never invents a DISARM identifier.

Change control

Entries change only through the quarterly Tradecraft Report, each revision carrying the old value, the new value, the rationale, and the editor. Superseded text stays reachable. A retired identifier stays retired, with its successor named.

The Families and Maneuvers

The tables below carry every maneuver in version 1.0, grouped by family. Family counts run from 6 to 9 because maneuvers anchored in Iranian and North Korean doctrine joined the original 54 during the build.

CW-F01 Narrative Engineering

Frame design, agenda seeding, and narrative laundering.

Doctrinal spread. Chinese public-opinion guidance and public-opinion warfare; Russian narrative laundering; general framing practice.

ID	Maneuver	Anchor	Definition
CW-M0006	Frame Pre-Seeding	Gen	Frame pre-seeding plants a narrative before the triggering event so the frame is ready when the event lands. The audience meets the event already primed to read it a set way.
CW-M0007	Narrative Laundering	RU	Narrative laundering moves a state-origin claim through fringe and proxy outlets until it re-enters mainstream discourse stripped of its Russian origin. The wash removes the fingerprint, not the message.
CW-M0008	Grievance Framing	Gen	Grievance framing casts a group as wronged to mobilize anger and loyalty. The wound, real or manufactured, becomes the organizing principle.
CW-M0009	Whataboutism Deflection	RU	Whataboutism deflection answers an accusation with a counter-accusation to level the moral ground. The pivot changes the subject rather than the facts.

ID	Maneuver	Anchor	Definition
CW-M0010	Historical-Analogy Anchoring	CN	Historical-analogy anchoring ties a present dispute to a charged national memory so audiences read the dispute through the older wound. The maneuver imports the emotion and the conclusion of the past event, not its facts.
CW-M0011	Manufactured-Consensus Framing	CN	Manufactured-consensus framing presents a contested claim as the settled majority view to shift the perceived center of opinion. The maneuver fabricates the appearance of agreement, not the agreement.
CW-M0055	Cultural-Invasion Framing	IR	Cultural-invasion framing casts foreign culture, media, and ideas as a coordinated attack on the nation and the faith, justifying mobilization and control. The threat frame, not any single claim, does the work.
CW-M0056	Resistance-Axis Narrative Projection	IR	Resistance-axis narrative projection pushes a single anti-Western and anti-Israel storyline across a network of front outlets and personas that appear independent. The network, not any one site, carries the reach.
CW-M0059	Ideological-Messaging Projection	DPRK	Ideological-messaging projection pushes regime ideology outward through united-front outlets and official statements directed at foreign and diaspora audiences. The message defends the regime line rather than winning an argument.

CW-F02 Amplification and Reach

Bot networks, coordinated inauthentic behavior, state-media tiering, and influencer capture.

Doctrinal spread. Russian three-tier amplifier model; Chinese Spamouflage output; general coordinated inauthentic behavior.

ID	Maneuver	Anchor	Definition
CW-M0003	Milblogger Amplification Layering	RU	Milblogger amplification layering moves a narrative from origination on Telegram military-blogger channels up through grey-zone proxies and state media to automated amplification, laundering pro-Kremlin content into Western feeds. Each tier adds reach and strips attribution.
CW-M0012	Bot-Network Amplification	Gen	Bot-network amplification runs automated accounts to inflate the reach and apparent popularity of a message. Volume manufactures a signal of consensus.
CW-M0013	Coordinated Inauthentic Posting	CN	Coordinated inauthentic posting runs clusters of fake or controlled accounts posting in concert to simulate organic support across many platforms. The coordination hides behind a mask of independent voices.
CW-M0014	Influencer Capture	Gen	Influencer capture recruits or pays genuine influencers to carry state-aligned messaging to their trusting audiences. The audience trust in the creator transfers to the message.
CW-M0015	Cross-Platform Seeding	Gen	Cross-platform seeding places the same content across many platforms at once to build resilience and an impression of independent spread. No single takedown removes the message.
CW-M0016	Hashtag Hijacking	Gen	Hashtag hijacking floods a trending or opposing hashtag to redirect its conversation or drown its signal. The tactic captures an existing audience rather than building one.

CW-F03 Persona and Front Operations

Synthetic personas, front organizations, and laundered experts.

Doctrinal spread. Chinese United Front front-group and overseas work; Russian persona operations; generative-AI persona tooling.

ID	Maneuver	Anchor	Definition
CW-M0017	Synthetic-Persona Operation	RU	Synthetic-persona operation fields fabricated individuals to carry messaging at scale. The invented person, not the argument, delivers the claim.
CW-M0018	Front-Media Establishment	RU	Front-media establishment stands up outlets that appear independent while under covert direction. The masthead is local; the principal is the Russian state.
CW-M0019	Expert Laundering	CN	Expert laundering routes state messaging through foreign credentialed voices to borrow their authority. The credential, not the argument, carries the claim.
CW-M0020	Front-Organization Fielding	CN	Front-organization fielding creates advocacy or civil-society groups that mask Party sponsorship. The civic form conceals the true principal.
CW-M0021	Sockpuppet Infiltration	Gen	Sockpuppet infiltration inserts fake personas into genuine communities to steer them from inside. The trusted-insider pose does the steering.
CW-M0022	Diaspora-Proxy Mobilization	CN	Diaspora-proxy mobilization activates co-ethnic and student networks to carry Party influence into a target society and to suppress dissent abroad. The proxy's local standing does the work the state avoids doing openly.
CW-M0057	False-Flag Persona Fielding	IR	False-flag persona fielding impersonates a real domestic group or individual to intimidate a target and misdirect blame. The borrowed identity, not the operator, carries the threat.

CW-F04 Forgery and Fabrication

Clone sites, forged documents, synthetic media, and staged events.

Doctrinal spread. Russian active measures, from Secondary Infektion to Doppelganger; general synthetic-media fabrication.

ID	Maneuver	Anchor	Definition
CW-M0002	Doppelganger Clone-Site Forgery	RU	Doppelganger clone-site forgery stands up lookalike copies of real news outlets and government domains to launder fabricated stories under a trusted masthead. The maneuver couples typosquatted domains and copied page furniture with fake personas and paid amplification.
CW-M0023	Document Forgery	RU	Document forgery fabricates or alters official-looking documents to seed a false claim. The forgery borrows the authority of the letterhead it counterfeits.
CW-M0024	Synthetic-Media Fabrication	Gen	Synthetic-media fabrication generates fake audio, video, or images to place false words or acts on a real person. The forgery wears a trusted face.
CW-M0025	Staged-Event Production	RU	Staged-event production either physically stages a scene for footage or brands a real event a fake to blunt its impact. The claim of staging becomes the payload.
CW-M0026	Fabricated-Poll Injection (provisional)	Gen	Fabricated-poll injection publishes invented polls or survey data to manufacture a perception of where opinion sits. The fake number sets an anchor the real debate then chases.
CW-M0027	Quote and Attribution Fabrication	Gen	Quote and attribution fabrication puts invented words in a real person's mouth or forges a document under a real name. The borrowed authority carries the lie.

CW-F05 Reflexive Control and Decision Shaping

Option shaping, inevitability framing, escalation signaling, and provocation baiting.

Doctrinal spread. Russian reflexive control from Lefebvre through Komov and Gerasimov; the provokatsiya lineage; general decision theory.

ID	Maneuver	Anchor	Definition
CW-M0001	Reflexive-Control Conditioning	RU	Reflexive-control conditioning feeds an adversary specially prepared information so the target chooses, of its own accord, the option the initiator prefers. The maneuver shapes the perception behind a decision rather than forcing the decision.
CW-M0005	Provocation-Overreaction Baiting	RU	Provocation-overreaction baiting stages or amplifies a provocation designed to draw a target overreaction, which then feeds a pre-planned narrative of repressive elites or Western authoritarianism. The manufactured event, not the target's genuine conduct, supplies the propaganda image.
CW-M0028	Inevitability Framing (provisional)	RU	Inevitability framing presents an outcome as unavoidable to induce concession and drain morale. The target is persuaded to quit, not to believe a fact.
CW-M0029	Escalation Signaling	RU	Escalation signaling projects an escalation threat decoupled from real posture to deter a decision. The signal is calibrated to the audience's fear, not to actual intent.
CW-M0030	False-Moderation Positioning (provisional)	Gen	False-moderation positioning pairs an extreme demand with a reasonable-looking fallback to move the perceived center toward the fallback. The extreme anchor makes the real ask look moderate.
CW-M0031	Decision-Paralysis Induction	RU	Decision-paralysis induction floods a decision-maker or public with contradictory accounts to stall a choice. Doubt, not any single version, is the objective.
CW-M0060	Belligerent Signaling	DPRK	Belligerent signaling issues calibrated threats through official statements and tests to shape an adversary's decisions. The statement targets the audience's fear rather than any fact.

CW-F06 Seam Exploitation

Platform-policy gaps, electoral timing, lawfare, and civil-liberty tension baiting.

Doctrinal spread. Chinese legal warfare; Russian wedge exploitation; general platform-governance gaming.

ID	Maneuver	Anchor	Definition
CW-M0032	Platform-Policy Gaming	Gen	Platform-policy gaming exploits the gaps and appeal processes in platform rules to keep an operation alive through enforcement. The rulebook becomes the shield.
CW-M0033	Electoral-Timing Exploitation	RU	Electoral-timing exploitation concentrates operations inside the narrow window before a vote, where correction has no time to catch up. The calendar, not the content alone, is the weapon.
CW-M0034	Lawfare Shielding	CN	Lawfare shielding uses legal claims, litigation, and legislation to legitimize the Party's position and to chill critics. The courtroom substitutes for the argument.
CW-M0035	Wedge-Issue Baiting (provisional)	RU	Wedge-issue baiting amplifies a society's most divisive issues from several sides at once to widen the fracture. The goal is heat, not any single position.
CW-M0036	Institutional-Trust Erosion	RU	Institutional-trust erosion attacks the credibility of elections, media, and courts so no shared account holds. The target is confidence itself, not a single institution.
CW-M0037	Jurisdictional-Gap Operation	Gen	Jurisdictional-gap operation routes an operation through states and services beyond the reach of the target's law. Distance from enforcement is the design.

CW-F07 Cyber-Cognitive Coupling

Hack-and-leak, disruption timed to narrative, and strikes staged as message.

Doctrinal spread. Russian GRU intrusion-plus-influence coupling; Iranian hack-and-leak; general destructive-signaling practice.

ID	Maneuver	Anchor	Definition
CW-M0004	Hack-and-Leak Narrative Coupling	RU	Hack-and-leak narrative coupling steals data through intrusion, then weaponizes it through a timed, framed release, whether real, altered, or salted with forgeries. The intrusion arm and the dissemination arm run as one operation.
CW-M0038	Disruption-Timed Messaging	RU	Disruption-timed messaging pairs a cyber disruption with a message addressed to the enemy population and leadership. The outage is the stage; the post is the line.
CW-M0039	Defacement Signaling	Gen	Defacement signaling replaces a site's content with a message to project reach and intimidate. The broken page is the billboard.
CW-M0040	Data-Weaponized Doxxing	IR	Data-weaponized doxxing releases or threatens to release stolen personal data to intimidate a target or mobilize harassment. Exposure itself is the weapon.
CW-M0041	Fabricated-Breach Claiming	RU	Fabricated-breach claiming inflates or invents a hack to project capability and fear. The claim, not the intrusion, does the cognitive work.
CW-M0042	Wiper-as-Message Operation	RU	Wiper-as-message operation stages destructive cyber action for its psychological effect, often behind a ransomware disguise. The destruction is the message, not the payoff.
CW-M0058	Perception-Projection Signaling	IR	Perception-projection signaling pairs limited cyber access with a message that inflates the breach into a larger threat. The impression of capability, not the access itself, is the objective.

CW-F08 Terrain Preparation

Audience mapping, grievance cultivation, diaspora targeting, and long-horizon media capture.

Doctrinal spread. Chinese United Front elite cultivation and long-horizon capture; Russian audience preparation; general targeting practice.

ID	Maneuver	Anchor	Definition
CW-M0043	Audience Mapping	Gen	Audience mapping profiles a target population to find the segments most open to influence. The map decides where the effort lands.
CW-M0044	Grievance Cultivation	Gen	Grievance cultivation nurtures a grievance community over time for later activation. The slow build is the investment.
CW-M0045	Long-Horizon Media Capture	CN	Long-horizon media capture acquires or co-opts global distribution years ahead of need, so the Party holds the channel before the message exists. The apparent independence of the outlet is the product being sold.
CW-M0046	Elite Cultivation	CN	Elite cultivation builds relationships with influential figures to shape future access and messaging. Capturing a few reaches the many they influence.
CW-M0047	Sleeper-Asset Placement	Gen	Sleeper-asset placement positions accounts, personas, or operatives to lie dormant until needed. The asset ages into credibility before it acts.
CW-M0048	Dependency Cultivation	CN	Dependency cultivation builds a target's informational and infrastructural dependence to gain a later hold. The dependence becomes the pressure point.
CW-M0062	Fraudulent-Worker Infiltration	DPRK	Fraudulent-worker infiltration places operatives inside foreign firms under stolen or invented identities to earn revenue and hold access. The false identity is the wedge.

CW-F09 Suppression and Denial

Flooding, harassment campaigns, discredit operations, and censorship export.

Doctrinal spread. Russian flooding practice; Chinese censorship export and access denial; general coordinated harassment.

ID	Maneuver	Anchor	Definition
CW-M0049	Information Flooding	RU	Information flooding saturates a channel to bury an inconvenient signal under sheer volume. Quantity, not any single claim, carries the effect.
CW-M0050	Coordinated Harassment	Gen	Coordinated harassment directs a swarm of accounts at a target to silence or intimidate them. The pile-on is the weapon.
CW-M0051	Discredit Campaigning	RU	Discredit campaigning attacks a source's credibility to neutralize its message. The person or body, not the evidence, becomes the target.
CW-M0052	Mass-Reporting Takedown	Gen	Mass-reporting takedown coordinates false abuse reports to trigger a platform into removing a legitimate account or post. The rules are turned against the target.
CW-M0053	Censorship Export	CN	Censorship export pressures foreign companies, platforms, and states to apply the Party's censorship beyond its borders. The rule travels farther than the regime that wrote it.
CW-M0054	Access Denial	CN	Access denial cuts a population's access to outside information through border filtering and shutdowns, and promotes that model as an exportable norm. Silence is imposed at the pipe, not the platform.
CW-M0061	Front-Channel Suppression	DPRK	Front-channel suppression removes or restructures the regime's own external outlets to enforce a new line. The withdrawal itself is the observable signal.

A Complete Entry

The entry below appears exactly as paid subscribers receive it. Every field the schema demands shows up, including the falsifier and the DISARM crosswalk.

CW-M0002 Doppelganger Clone-Site Forgery

Family: CW-F04 Forgery and fabrication

Aliases: Doppelganger; RRN (Recent Reliable News); Ruza Flood; Storm-1099.

Definition. Doppelganger clone-site forgery stands up lookalike copies of real news outlets and government domains to launder fabricated stories under a trusted masthead. The maneuver couples typosquatted domains and copied page furniture with fake personas and paid amplification.

Doctrinal lineage. The operational doctrine sits in the Soviet active-measures tradition of dezinformatsiya, updated for the web. Primary adversary material is unusually direct: the FBI seizure

affidavit of September 4, 2024 (Case 2:24-mj-01395, Eastern District of Pennsylvania) quotes the Social Design Agency's own internal strategy and tasking documents, adversary primary text obtained through seizure. The operational lineage runs through InfoRos in the 2000s, Secondary Infektion from 2014, and Portal Kombat in 2023. Thomas Rid's Active Measures supplies secondary historical framing.

Observable indicators, ranked.

Rank	Indicator	Specificity
1	Typosquatted lookalike domains (bild.llc, spiegel.ltd, washingtonpost.pm, diplomatie.gouv.fm)	High
2	Cloned CSS and copied cookie-consent banners	High
3	Shared web-analytics account IDs across successor domains	High, forensic
4	Cloaked geofenced redirect chains	High
5	Machine-translation artifacts and reused image filenames	Moderate

Exemplar cases.

Case	What happened	ASA tri-score	Grade
Initial exposure, September 27, 2022	EU DisinfoLab and Qurium documented cloned Süddeutsche Zeitung and other outlets pushing "sanctions must end" narratives.	T Strong / D Low / F Likely	B2
VIGINUM RRN report, June 19, 2023 (FR) / July 19, 2023 (EN)	France's technical service documented at least 49 false Le Parisien articles and a forged Foreign Ministry document on the diplomatie.gouv.fm subdomain.	T Solid / D Low / F Likely	A2
US action, March 20 and September 4, 2024	Treasury designated Gambashidze, Tupikin, the SDA, and Structura; the Justice Department seized 32 domains and revealed a list of roughly 2,800 influencers.	T Solid / D Low / F Likely	A1

Actor instantiation. The Social Design Agency and Structura National Technology run the operation under the Presidential Administration, specifically First Deputy Chief of Staff Sergei Kiriyenko; Ilya Gambashidze and Nikolai Tupikin are the named principals. The maneuver anchors Russia's **Cognitive Warfare Velocity 88** and **Narrative Volume 89**, and draws on **AI Tradecraft Adoption 82** through the CopyCop and Storm-1516 machine-generated site expansion. Composite Russia 85, Tier 0.

Adversary claims, separated. Doppelganger stays conspicuously absent from Russian state-media archives; Novaya Gazeta Europe reports an editorial block on naming it. One Meta-exposed network claimed a Russian-intelligence contract for the Stars-of-David stencil operation. The self-claim stays apart from the verified attribution.

Detection signatures. Shared analytics IDs; link cloaking; translation artifacts; reused image filenames; the AEZA bulletproof-hosting nexus.

Countermeasures.

Countermeasure	Graded feasibility
Domain seizures	Feasible but partial; domains persisted a month after the September 2024 seizures
OFAC and EU sanctions	Feasible, slow
Platform takedowns	Feasible
Ad-network moderation	Moderate

Falsifier. DFRLab (October 9, 2024) found seized domains back online within a month through shared infrastructure, and little organic social reach. A sustained collapse of successor infrastructure after a seizure, rather than the observed persistence, breaks the resilient-laundering reading. Absence of the typosquat-plus-cloned-furniture pairing places a case outside the maneuver.

DISARM crosswalk.

DISARM ID	Technique name	Note
T0143.003	Impersonated Persona	Replaces the deprecated legacy T0099
T0097.202	News Outlet Persona	Cloned masthead identity
T0097.206	Government Institution Persona	Forged ministry identity
T0098	Establish Inauthentic News Sites	The clone network itself
T0149.003	Lookalike Domain	Typosquatted registration
T0089.003	Alter Authentic Documents	The forged ministry document

Change log. v1.0. July 17, 2026. First draft against primary tasking documents in the DOJ affidavit. Template locked. v1.1. September 21, 2026. Storm-1679 removed from aliases; Microsoft tracks it as a separate actor, and Ruza Flood is Microsoft's name for Doppelganger.

What the Paid Tiers Hold

The free edition shows the taxonomy and the method. Three subscriber tiers carry the evidence.

Tier	What it holds
Tier 1 · Analyst	All 62 maneuvers at full fifteen-field depth, with graded exemplars, actor instantiations, detection signatures, countermeasures, falsifiers, and DISARM crosswalks; all 107 techniques; the full quarterly Tradecraft Report
Tier 2 · Institutional	Everything in Tier 1, plus the AI-Enabled Influence Production Register and the complete DISARM crosswalk and gap register; the actor-by-maneuver matrix for 38 ranked actors arrives across the January and April 2027 reports
Tier 3 · Executive Desk	Everything in Tier 2, plus named-analyst review, a pre-release briefing on each Tradecraft Report, falsifier watch, and counter-playbooks from January 2027

Table 4. Subscriber tiers of the Reference.

Pricing and briefings are available on request. Write to info@treadstone71.com or visit www.treadstone71.com.

Using the Reference

Cite a maneuver by identifier and name, with the version: CW-M0002 Doppelganger Clone-Site Forgery, Cognitive Warfare Tradecraft Reference version 1.0. Identifiers stay stable across versions, so a citation written today resolves next year.

Challenge a name, a definition, or a family boundary. Public or private, either works. The quarterly Tradecraft Report answers the ones that change the Reference, and its falsifier section reports where the Reference got something wrong.

Terms of Use

© 2026 Treadstone 71. The Tier 0 Free Edition circulates freely. Read it, share it, and cite it with attribution to Treadstone 71 and a link to www.treadstone71.com. Reproduction for commercial use, resale, or modified versions requires written permission from Treadstone 71. Other work is welcome to use the identifiers and definitions, cited to the Reference and its version.