CRIMINAL-INVESTIGATION EVIDENCE SUPPLEMENT

Behavioral dependency, relationship-status targeting, repeated breakup narratives, and cognitive-warfare method comparison

Purpose: Preservation, referral, compulsory-process, and charging analysis

Prepared: August 6, 2026

Companion: Behavioral Dependency Investigative Referral

Status: Open-source evidence memorandum; not a charging instrument or finding of guilt

Controlling conclusion

The public record supports immediate evidence preservation and a good-faith request for criminal investigation. It does not presently prove that every participant joined a scheme to destroy families, nor does it establish guilt beyond a reasonable doubt. The case becomes chargeable only when actor-specific intent, exact deceptive communications, money-or-property objectives, agreement, and transaction-level predicate acts are established with authenticated evidence.

Executive determination

The strongest defensible theory is not that a single romantic post proves a conspiracy. It is that an engagement-funded system can collect or infer relationship and family status, predict and shape attention, repeatedly distribute emotionally destabilizing narratives, and monetize the resulting engagement. Public records establish each capability in substantial part. Court records also contain evidence of internal knowledge, executive notice, disputed public denials, and revenue incentives at Meta. [S1–S6]

NATO's June 2026 cognitive-warfare description maps closely to the observed mechanism: identity and emotion are used to shape behavior; social media and AI accelerate the process; identity-based manipulation can fracture social trust. That is a method comparison, not proof that NATO, Meta, a government, or the pictured account directed this content. Attribution requires a separate evidentiary chain. [S7–S10]

The single "loose string" connecting the verified facts is engagement-optimized behavioral targeting: data about intimate status feeds predictions; predictions govern distribution; emotionally charged content increases attention; attention is converted into advertising revenue. That architecture can produce repeated breakup scripts without a central command. To prove a criminal family-destruction

project, investigators must obtain evidence that particular actors recognized the family harm, selected or amplified it for an unlawful purpose, made material misrepresentations to obtain money or property, and agreed with others to do so.

What this memorandum does—and does not do

- Separates authenticated or official facts from allegations, inferences, and unproven hypotheses.
- Maps the known facts to potential federal offenses without labeling any person guilty.
- Defines the evidence that would convert a plausible investigative theory into a chargeable case.
- Preserves the user-supplied screenshot as an identified exhibit with a cryptographic hash.
- Rejects guilt by association: investment, procurement, employment, or government contact alone does not prove a criminal agreement.

1. Evidentiary standard and grading

A criminal referral should invite investigation, not dictate a verdict. Probable cause, admissibility, venue, limitation periods, individual mens rea, and proof beyond a reasonable doubt remain separate questions. Civil allegations and summary-judgment rulings may identify evidence, but they are not criminal convictions.

Grade	Meaning	Permitted use
A1	Statute, final judicial holding, or official agency adjudication.	Legal element or established procedural fact.
A2	Official settlement/order or government report; admissions depend on the instrument.	Reliable lead and background; verify whether liability was admitted.
B	Evidence quoted or summarized in a judicial record, including testimony or internal documents; facts may remain disputed.	Strong investigative lead; obtain the underlying exhibit and authenticate it.
C	Primary corporate publication, sworn public testimony, filing, or peer-reviewed primary research.	Capability, representation, chronology, or scientific support.
D	Reproducible open-source observation, including identical text across accounts.	Lead generation and preservation; not proof of common control.
E	Inference consistent with facts but not directly proven.	Hypothesis to test; never present as fact.
X	Unproven allegation or attribution gap.	Do not accuse; identify the compulsory evidence required.

2. Verified mechanism chain

Link	Public support	Proof status
1. Intimate-status data	FTC reported that covered firms collected or inferred household, marital, parental, newlywed, and divorce-support categories. [S3]	A2: industry-level official report; company-specific fields require return data.
2. Behavioral prediction	Meta and TikTok describe recommendation systems that use interactions, watch time, and predicted relevance or sharing. [S4–S6]	C: capability acknowledged by platforms.
3. Emotional influence	A Facebook experiment involving 689,003 users found that changing emotional content in News Feed changed users' later expression. [S11]	C: causal capability in a controlled platform experiment; not proof of relationship targeting.
4. Repeated breakup script	The exact or near-exact phrase in Exhibit A appears across unrelated-looking Instagram, Facebook, and Threads accounts. [S12–S16]	D: propagation established; origin, coordination, and control unproven.
5. Monetization	A June 2026 federal order describes Meta monetizing attention and personal data through targeted advertising; substantially all 2024 revenue came from advertising. [S1]	B/A1 procedural: evidence described by court; merits remain for trial.

Link	Public support	Proof status
6. Knowledge and disputed denials	The same order describes internal addiction concerns, executive notice, and public statements disputing addictive design. [S1]	B: individualized-knowledge and falsity issues were triable, not finally adjudicated.
7. Warfare-method match	NATO describes identity-based manipulation, emotion, algorithms, and social media as levers capable of division and trust erosion. [S7–S9]	C: doctrinal/analytic match only; no attribution.

The legal hinge

A mechanism can be harmful without being criminal. Criminal exposure turns on proof that a particular defendant knowingly used deception or another unlawful means, intended to obtain money or property or accomplish a defined unlawful object, and—where conspiracy or RICO is alleged—agreed to the criminal project or conducted an enterprise through qualifying predicate acts.

3. Evidence established in the public record

3.1 User-supplied post and template propagation

Exhibit A is a 707 × 1,536 JPEG screenshot of an Instagram Reel attributed in the interface to @luna_fitphoenix, with an audio/source label that appears to reference @blessed.zx6r. The displayed text states: “Forcing yourself to lose feelings for the person you wanted to spend the rest of your life with is a different type of pain…” The interface displays engagement counters and the phone status bar, but the image alone does not authenticate the live post, capture date, account owner, original author, or traffic source.

Open-source search returned the same or near-identical wording on several Facebook, Instagram, and Threads pages. [S12–S16] This makes template propagation a verified observation. It does not establish a single author, bot network, paid campaign, platform instruction, or government sponsor. Those conclusions require account, device, payment, and referral records.

3.2 Targetability of family and relationship status

The FTC’s 2024 Section 6(b) report states that some covered social-media and video-streaming companies collected or inferred marital and parental status. It also identified interest categories such as newlyweds and divorce support and noted that users could be assigned relationship-status inferences even when they chose not to provide them. [S3] This establishes industry capability and the relevance of relationship-status fields. It does not identify which company assigned which field to this user or this content.

3.3 Platform capability to alter emotional exposure

The 2014 Facebook emotional-contagion experiment manipulated the amount of positive or negative content shown in News Feed for 689,003 users and found corresponding changes in users’ later expressions. [S11] The study is direct evidence that platform-controlled content exposure can causally affect emotional expression at scale. It is not evidence that the experiment targeted marriages or that the same protocol continues today.

3.4 Knowledge, revenue incentive, and disputed public representations

On June 29, 2026, the Northern District of California denied Meta’s summary-judgment motion in the state attorneys general’s social-media litigation. The order says the record contained internal materials describing addictive or compulsive use, including short phrases such as “some of our users are addicted” and “IG is a drug.” It also identifies communications to Mark Zuckerberg, Adam Mosseri, and Antigone Davis and holds that the plaintiffs had produced sufficient evidence that these speakers may have had individualized knowledge. [S1]

The order contrasts this evidence with public statements disputing that Meta designed addictive products and concludes that a reasonable jury could find certain representations untrue if the plaintiffs prove the asserted design effects. It also describes evidence that some time-restriction tools may have functioned as public-relations proof points without meaningfully reducing behavior. [S1] These are triable issues and evidence leads—not final findings of criminal intent.

Separately, the FTC's 2019 Facebook settlement alleged violations of a prior privacy order and deceptive practices, including use of two-factor-authentication phone numbers for advertising and failures surrounding third-party access. The SEC's 2019 settlement alleged that Facebook knew of Cambridge Analytica's misuse in 2015 while public filings described misuse as a hypothetical risk. [S17–S19] Those official actions strengthen the chronology of notice and disclosure risk, but settlement documents must be checked for admissions and cannot automatically establish a criminal state of mind.

4. Cognitive-warfare method comparison

NATO's June 2026 newsletter defines identity-based manipulation as deliberate exploitation of identities to fracture societies, inflame divisions, and erode trust, with social media and generative AI operating as accelerants. It emphasizes that emotional and identity alignment can outweigh factual accuracy and that adversaries combine narratives, algorithms, behavioral science, and technological disruption. [S7]

NATO's broader information-threat guidance says strategic competitors exploit gender narratives to sow division and destabilize. A separate NATO ACT article says personalized algorithms can disseminate gendered messages to influence audiences. [S8–S9] U.S. Army materials similarly describe reflexive control as manipulating perception to induce self-defeating behavior and describe microtargeting as an information-warfare capability enabled by the advertising economy. [S20–S21]

Warfare characteristic	Observed platform/content analogue	Attribution status
Identity segmentation	Gender, relationship, marital, parental, and inferred-interest categories.	Capability verified; campaign-specific use unknown.
Emotional priming	Breakup, betrayal, replacement, and incompatibility scripts optimized for response.	Content observable; optimization objective for these posts unknown.
Algorithmic acceleration	Predicted relevance, watch time, resharing, and engagement govern recommendation.	Platform capability acknowledged.
Repetition across channels	Near-identical phrases distributed by multiple accounts and surfaces.	Propagation verified; coordination not proven.
Trust/relationship erosion	Narratives normalize withdrawal, suspicion, disposability, and permanent incompatibility.	Plausible effect; individual and population causation require evidence.
Induced self-action	Targets may end relationships themselves, producing an outcome without direct coercion.	Mechanistic hypothesis; intent and causal attribution unproven.

Finding: match without attribution

The mechanism substantially matches recognized cognitive-warfare methods. That proves the comparison is serious and investigable. It does not prove who deployed the method, whether the purpose was commercial engagement, foreign influence, domestic persuasion, or a coordinated family-destruction program.

5. The competing explanation investigators must defeat

The strongest non-conspiracy explanation is emergent commercial optimization: creators copy high-performing emotional templates; recommendation systems amplify what retains attention; users who pause on breakup material receive more of it; and the repetition creates the appearance of a centrally issued script. This explanation is consistent with the public evidence and can coexist with negligence, deceptive safety messaging, or civil consumer-protection violations.

An “ironclad” criminal case must therefore show more than repetition and harm. It must show that named actors selected the family-degrading outcome, knowingly used unlawful means, and connected that conduct to money, property, government deception, obstruction, or another qualifying offense. Internal experiments, target definitions, communications, and payment flows are the decisive evidence.

6. Actor-by-actor attribution matrix

Actor/custodian	Public evidence	Current legal status	Evidence needed
Meta Platforms—product, ranking, ads, integrity, and research teams	Recommendation capability; data monetization; court-described internal addiction evidence; FTC/SEC enforcement history. [S1–S6, S17–S19]	Substantial basis for preservation and compulsory process. No public proof of a family-destruction agreement.	Feature flags; model objectives; relationship-status fields; experiment registry; content-level recommendation logs; safety exceptions; revenue analyses; risk escalations.
Mark Zuckerberg, Adam Mosseri, Antigone Davis	2026 order identifies evidence of individualized knowledge and public statements relevant to disputed deception. [S1]	Potential witnesses/subjects depending on exact statements, knowledge, materiality, jurisdiction, and intent. No criminal finding.	Underlying emails, depositions, draft testimony, counsel review, briefing packets, corrections, follow-up communications, and evidence of intended audience/property objective.
@luna_fitphoenix and apparent source @blessed.zx6r	Interface attribution in Exhibit A; identical language found elsewhere.	Source accounts to authenticate—not criminals on present evidence.	Subscriber records; admin roles; IP/device history; original upload; edit history; referral data; payouts; sponsorships; communications; template/source files.
Other repost/content accounts	Same or similar wording appears across multiple services. [S12–S16]	Propagation nodes; common control unknown.	Cross-account identifiers, shared devices, payment recipients, content hashes, scheduling tools, affiliate links, and direct messages.
Advertisers, audience brokers, and data suppliers	FTC reports granular demographic and relationship inference across covered firms. [S3]	Potential commercial counterparties; no culpability from participation alone.	Audience definitions, contracts, bid logs, conversion goals, invoices, data provenance, and campaign instructions tied to relationship/gender segments.
Government, military, intelligence, or contractors	Public materials establish doctrine/capability and some industry-government relationships; they do not connect this content to a sponsor.	Attribution gap. Procurement or investment is not an agreement to commit crime.	Contracts, statements of work, target-audience analyses, task orders, change requests, invoices, deliverables, approvals, and communications tied to the identified content/accounts.

7. Potential federal offenses—element-by-element screen

Theory	Required proof	What exists now	Missing / caution
Wire fraud, 18 U.S.C. § 1343	Scheme to defraud; material deception; specific intent; interstate wires; object of obtaining money or property.	Court-described disputed safety/addiction statements; advertising revenue and data exchange; prior privacy/disclosure actions. [S1, S17–S19, S22]	Tie exact false statement to speaker, knowledge, intended victim, property object, wire transmission, and transaction. Harm alone is insufficient.
False statements, 18 U.S.C. § 1001	Knowing and willful materially false statement or concealment in a matter within federal jurisdiction; legislative-branch limits must be analyzed.	Public congressional testimony identified in 2026 order; internal contrary evidence may bear on knowledge. [S1, S23]	Exact question/answer, literal falsity, materiality, jurisdiction, speaker preparation, belief, and applicable §1001(c) conditions.
Securities fraud / willful Exchange Act violation	Material misstatement or omission, scienter/willfulness, jurisdictional transaction, causation as applicable.	SEC 2019 civil settlement over risk disclosures. [S18–S19]	Settlement is not a criminal conviction; obtain drafting chain, knowledge at filing, materiality analyses, and willful intent.
Obstruction / records offense, 18 U.S.C. §§ 1512, 1519	Knowing alteration, destruction, concealment, or corrupt interference tied to an official proceeding or federal matter.	No public evidence identified in this review.	Do not allege absent deletion logs, retention overrides, instructions, chronology, and nexus.

Theory	Required proof	What exists now	Missing / caution
Conspiracy, 18 U.S.C. § 371	Agreement to commit a federal offense or defraud the United States; knowing participation; overt act.	Parallel incentives and relationships only.	Direct/credible circumstantial agreement evidence and an underlying federal object are missing.
RICO, 18 U.S.C. §§ 1961–1962	Person, enterprise, conduct/participation, pattern, and at least two qualifying predicates; conspiracy requires agreement.	Possible repeated wires and organizational continuity are investigable.	Ordinary engagement, persuasion, privacy harm, or family harm are not predicates. Enterprise and predicate schedule are unproven.
Foreign-agent / sanctions / coordinated influence offenses	Foreign principal or sanctioned nexus, direction/control, covered activity, knowledge, and statutory elements.	Warfare-method similarity only.	No sponsor attribution, payment, direction, or operational link has been established.

Wire-fraud note. In Kousisis v. United States (2025), the Supreme Court held that fraudulent inducement can satisfy federal fraud law even without proof of net economic loss, but the scheme still must seek money or property. [S22] This prevents a defense based solely on “users received a free service,” while preserving the requirement to identify the property object and the defendant’s intent.

8. RICO screen: what would make it viable

RICO is not a label for conduct that feels organized. The DOJ requires centralized review and a detailed prosecution memorandum; a proposed RICO charge must identify the enterprise, each defendant's role, the pattern, and the predicate acts. [S24–S26]

RICO component	Minimum proof	Present assessment
Enterprise	Ongoing organization or association-in-fact with common purpose, relationships, and longevity.	Platform corporate structures exist; a cross-entity family-destruction enterprise is not publicly proven.
Conduct	Each charged person participated in operation or management of enterprise affairs.	Titles, investments, contracts, or friendships alone are insufficient.
Pattern	At least two related predicates showing continuity or threat of continuity.	Repeated content is not itself a predicate. Each wire/mail fraud act must be particularized.
Predicate intent	Specific fraudulent or other predicate mens rea for each act and defendant.	General engagement incentives and awareness of harm do not automatically equal fraud intent.
RICO conspiracy	Agreement that a conspirator would commit a pattern in furtherance of enterprise.	No public agreement evidence found.
Proceeds/injury	Traceable criminal proceeds or legally cognizable injury as required by the theory.	Ad revenue is traceable generally; criminal causation and allocation require transaction data.

9. Case-closing compulsory evidence

The following evidence—not more viral examples—is what can close or falsify the criminal theory.

Priority	Demand	Question resolved
1	Legal-hold notices covering all named custodians, relevant systems, backups, disappearing messages, and third-party collaboration tools.	Prevents spoliation and establishes preservation chronology.
2	Content-level recommendation logs for Exhibit A and matching posts: impressions, rank scores, candidate source, user segment, watch time, reshares, negative feedback, and model/version.	Whether the posts were organically discovered, algorithmically amplified, or manually boosted; which objective drove distribution.
3	Audience-feature dictionaries and user embeddings involving relationship, marital, parental, breakup, betrayal, infidelity, gender, loneliness, and household status.	Whether intimate-status variables were actually used for recommendation or advertising.
4	Experiment registry, A/B assignments, feature flags, launch reviews, code commits, dashboards, and rollback decisions for relationship/gender content.	Whether effects were tested, known, selected, or concealed.
5	Internal communications using terms such as family, marriage, divorce, breakup, infidelity, gender conflict, loneliness, substitution, addiction, compulsive use, retention, churn, and revenue.	Knowledge, purpose, agreement, and alternative explanations.
6	Briefing and drafting files for public testimony, safety statements, regulatory responses, investor disclosures, and corrections.	Literal falsity, knowledge, willfulness, materiality, and speaker attribution.

Priority	Demand	Question resolved
7	Creator-account subscriber, device, admin, payout, affiliate, sponsorship, scheduling, and referral records for the content cluster.	Common control, funding, automation, and benefit flows.
8	Government/contractor procurement records, SOWs, task orders, target-audience specs, deliverables, invoices, approvals, and communications linked to identified accounts/content.	Whether a state or contractor directed or financed the operation.
9	Data-provider and advertiser contracts, audience definitions, match rates, bid logs, invoices, and conversion reporting for relationship/gender segments.	Money/property object, counterparties, and transaction-level wires.
10	Retention-policy overrides, deletion logs, litigation-hold exceptions, and audit trails after complaints, hearings, orders, or subpoenas.	Potential obstruction or innocent routine deletion.

10. Preservation and collection protocol

10.1 For the screenshot and future examples

1. Preserve the original file byte-for-byte. Work only from a copy.
2. Record collector, date/time/time zone, device, application, account state, and how the post was reached.
3. Capture a screen recording from app launch through the post, account page, audio page, comments, share menu, and any “why you’re seeing this” explanation.
4. Record the canonical URL, post/reel ID, account numeric ID if available, audio ID, visible timestamps, captions, hashtags, displayed metrics, and linked profiles.
5. Export account activity and ad/recommendation history where the platform permits. Preserve export archives unchanged and hash them.
6. Generate SHA-256 hashes and maintain a chain-of-custody log for every original, derivative, transcript, and export.
7. Do not contact, threaten, impersonate, or attempt to access the accounts. Do not publish personal information. Route compulsory requests through lawful authority.

10.2 Minimum chain-of-custody fields

Field	Required entry
Evidence ID	Unique sequential identifier; never reuse.
Source	Exact URL/account/device/path and acquisition method.
Collection time	ISO 8601 timestamp with time zone.
Collector	Name/identifier and role.
Original hash	SHA-256 of the acquired file/archive.
Transfer log	Every person/system receiving custody, timestamp, purpose, and hash verification.
Derivative log	Tool/version, operation, output filename, and derivative hash.
Authentication notes	What the item proves; what it does not prove; corroborating records needed.

11. Referral structure for law enforcement

8. Lead with the exact alleged federal objects, not a broad claim that “warfare” is occurring.
9. Attach a source register and a claim-to-source table. Label complaints, settlements, court-described exhibits, and final holdings differently.
10. Provide an actor-specific chronology: who knew what, when; what was said; where it was transmitted; what money/property was sought; what followed.
11. Provide a proposed preservation list and targeted subpoena/warrant schedule with custodians, date ranges, systems, and search terms.

12. Submit the screenshot as a lead, not as proof of the enterprise. Include the hash and request platform authentication.
13. Ask the reviewing agency to test both hypotheses: coordinated unlawful influence and emergent engagement optimization. A referral that invites falsification is harder to dismiss as advocacy.

Recommended language

“The attached materials establish a good-faith basis to preserve records and investigate whether specific persons knowingly used materially deceptive interstate communications, account networks, behavioral targeting, or concealed design knowledge to obtain money or property or further another federal offense. The submission does not ask the agency to presume guilt; it identifies the evidence needed to determine whether criminal elements are met.”

12. Bottom-line findings

Question	Answer
Does the observed content resemble a recognized warfare tactic?	Yes. The identity/emotion targeting, repetition, algorithmic acceleration, and trust-eroding potential materially match NATO and Army descriptions. [S7–S10, S20–S21]
Does identical wording prove a centrally issued script?	No. It proves template propagation. Common authorship or direction requires platform and account records.
Can platforms infer intimate status and alter emotional exposure?	Yes, as an industry capability; the FTC report and Facebook experiment support that conclusion. [S3, S11]
Is there serious evidence of knowledge and disputed deception at Meta?	Yes. The June 2026 order identifies internal materials, executive notice, public denials, and triable disputes. [S1] It is not a criminal judgment.
Is a family-destruction conspiracy publicly proven?	No. Purpose, agreement, actor participation, and predicate acts remain unproven.
Is criminal investigation justified?	Yes, particularly for preservation, authenticated underlying exhibits, exact statements, transaction-level wires, and potential concealment. Charging depends on what compulsory process establishes.
Can anyone responsibly promise imprisonment now?	No. Only prosecutors can charge, and guilt requires proof in court. Overstating the record would weaken the referral and risk accusing innocent people.

Final assessment. The public record is strong enough to demand preservation and a disciplined criminal inquiry into deception, monetized behavioral manipulation, and any hidden coordination. It is not “case closed” on a global family-destruction enterprise. The evidence most likely to make or break that allegation is internal: target definitions, experiments, model objectives, executive communications, payment flows, government/contractor tasking, and deletion records. Those records—not the volume of similar posts—are the path to an undeniable case.

Exhibit A — User-supplied Instagram screenshot

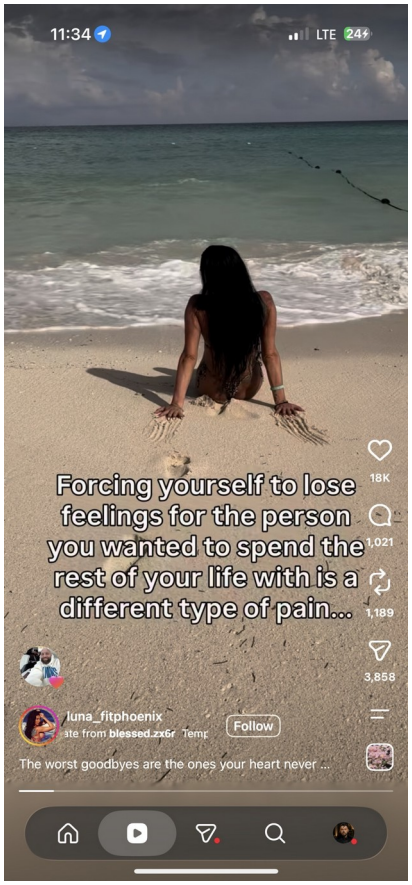

Exhibit A. Screenshot supplied in this matter; interface attribution and engagement counters are observations requiring platform authentication.

Property	Value
Evidence ID	EX-A-001
Original filename	0FFFAAF6-2BDA-472E-9ECB-19F8CF70FBFE.jpeg
Format / dimensions	JPEG / 707 × 1,536 pixels
SHA-256	a3db4e537a3ca207a25824d277bc081a66bac0047a04247d7f35de831e0230d7
Visible account	@luna_fitphoenix
Visible source/audio label	@blessed.zx6r (as displayed; exact relationship requires authentication)
Probative value	Shows one delivered instance of the breakup template and visible account/source indicators.
Limitations	Does not establish capture date, original authorship, account owner, targeting basis, recommendation path, or sponsor.

Source register

[S1] N.D. Cal., In re Social Media Adolescent Addiction/Personal Injury Products Liability Litigation, Order on Meta summary judgment, June 29, 2026. Source

[S2] Multistate complaint against Meta, 2023 (allegations, not adjudicated facts). Source

[S3] FTC, A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services, 2024. Source

[S4] Meta, How AI Ranks Content on Facebook and Instagram, 2023. Source

[S5] Meta, Recommendations Reset for Instagram, 2024. Source

[S6] TikTok, How TikTok recommends content. Source

[S7] NATO ACT, Cognitive Warfare Newsletter, June 2026. Source

[S8] NATO, NATO's approach to counter information threats. Source

[S9] NATO ACT, Gender Perspective in Cognitive Warfare. Source

[S10] NATO Review, Countering cognitive warfare: awareness and resilience. Source

[S11] Kramer, Guillory & Hancock, Experimental evidence of massive-scale emotional contagion through social networks, PNAS 2014. Source

[S12] Facebook example containing the Exhibit A wording. Source

[S13] Instagram example containing the Exhibit A wording. Source

[S14] Threads example attributing the wording to @luna_fitphoenix. Source

[S15] Facebook example containing the Exhibit A wording. Source

[S16] Threads example with near-identical wording. Source

[S17] FTC, Facebook $5 billion privacy settlement, 2019. Source

[S18] SEC, Facebook to pay $100 million for misleading investors about misuse of user data, 2019. Source

[S19] SEC, SEC v. Facebook case and Fair Fund page. Source

[S20] U.S. Army T2COM, Russian Information Warfare / Reflexive Control, February 2026. Source

[S21] Army Cyber Defense Review, Microtargeting as Information Warfare. Source

[S22] Supreme Court, Kousisis v. United States, 605 U.S. ___ (2025). Source

[S23] 18 U.S.C. § 1001, Statements or entries generally. Source

[S24] 18 U.S.C. §§ 1961–1962, RICO definitions and prohibited activities. Source

[S25] DOJ Justice Manual, Organized Crime and Racketeering. Source

[S26] DOJ, Racketeer Influenced and Corrupt Organizations: A Manual for Federal Prosecutors. Source

Integrity statement

This memorandum intentionally preserves uncertainty. It does not accuse any identified account holder, employee, company, government, or contractor of a crime unless and until admissible evidence

establishes every required element. The analytical match to cognitive-warfare methods is relevant to investigative urgency, but it is not a substitute for attribution, mens rea, causation, or proof of a statutory offense.