THESIS BRIEF — THEORY-FIRST RESEARCH

Edition: 2025-11-08 | Peer-review pending (Theory-First)

Smart Technology Investments

Cognitive Wars: the AI Industrialization of Influence

Nov 01–Nov 08, 2025 | Sources: 1 | Anchor Status: Anchor-Sparse | Report Type: Theoretical Research | Horizon: Near-term | Confidence: 0.800*

SD	AC	MT	RR
0.80	1.00	0.70	0.65

Alignment: 6.0 Theory Depth: 6.0 Clarity: 7.0

Disclosure & Method Note: This is a *theory-first* brief. Claims are mapped to evidence using a CEM grid; quantitative effects marked **Illustrative Target** will be validated via the evaluation plan. Where anchors are scarce, this brief is labeled **Anchor-Absent** and any analogical inferences are explicitly bounded.

Abstract & Theory-First Framing.

Outline

Theory-First Framework

Theory precedes description: we develop a causal model linking industrialization to cognitive dimensions of war. "Cognitive wars" are defined as organized campaigns that target populations' information environments and psychological states to alter beliefs, preferences, and decisions relevant to political or military objectives. Core variables and causal pathways:

- Production & Communication Capacities: physical throughput (printing presses, telegraph, radio, digital pipelines) that determine reach and latency.
- State–Society Integration: bureaucratic capacity, literacy, and mass education that create shared referents and centralized channels.
- Organizational Form & Coordination: industrial hierarchies and firms that enable scalable, repeatable influence operations.
- Feedback Loops in Belief Systems: success in cognitive operations produces institutional incentives to invest and optimize further.

Causal pathway (high level): industrialization -> expanded communication + integrated institutions -> scalable narratives and targeting -> persistent cognitive campaigns -> institutionalization of cognitive warfare.

Literature Review: Cognitive Wars

This review synthesizes interdisciplinary literatures: information warfare, propaganda and PSYOP studies, computational propaganda, and political psychology. Key observations:

- Historical scholarship documents state propaganda and mass mobilization in the industrial era; social scientists analyze persuasion, opinion dynamics, and mass communication effects.
- Recent computational work highlights automated amplification and the role of network structure in information diffusion.
- Gaps: many studies treat cognitive phenomena as auxiliary to kinetic capability rather than as structurally shaped by industrial and organizational conditions.

Relevant traditions: political psychology (attitude/behavior change), sociology of knowledge (institutional production of belief), network science (diffusion and consensus), and military studies (strategic communications, PSYOP).

Foundations

Why these anchors?

Selection strategy prioritizes peer-reviewed, non-preprint anchors for core methodological and theoretical touchstones; when such anchors are absent for a specific subtopic, canonical papers from broader abstraction layers are used to ground first-principles reasoning. In the present compilation, one peer-reviewed anchor (an ACM conference paper on consensus and adversaries) serves as a methodological touchstone for modeling distributed belief dynamics and adversarial influence processes [2]. Preprint and technical reports (graph-consensus literature) provide supplementary mathematical structure for networked opinion models [1].

Direct Sources (Layer 1)

- Contemporary studies describing computational propaganda, social bots, and synthetic media give empirical touchpoints for current AI-driven influence practices.

Domain Sources (Layer 2)

- Political communication and military PSYOP literatures place cognitive campaigns within strategic doctrine and historical practice.

Foundational Sources (Layers 3–4)

- Network science, information theory, and game theory supply formal tools for modeling diffusion, capacity limits, and adversarial equilibria.

Why include tangential canonical papers?

Canonical works from foundational layers—e.g., consensus and threshold models, and equilibrium game theory—are tangential to the empirical specifics of cognitive warfare yet provide essential primitives (information propagation, agent updating rules, adversarial optimization). These primitives permit principled extrapolation from industrial-era mechanisms to algorithmic-era dynamics, linking mechanistic models to historical and contemporary observations.

Theoretical Grounding and Conceptual Framework

Abstraction layers and concepts

- Layer 4 (Foundational): information theory (channel capacity, noise), statistical learning (generalization, adversarial examples), game theory (strategic interaction, equilibria), and network science (connectivity, centrality).
- Layer 3 (Abstract): social influence and persuasion (thresholds, conformity), opinion dynamics (consensus models, DeGroot-style averaging), and diffusion processes on networks (contagion vs. complex contagion).
- Layer 2 (Domain): organized influence—PSYOP, strategic communications, computational propaganda—characterized by target selection, narrative design, and amplification strategies.
- Layer 1 (Specific): cognitive warfare artifacts—automated disinformation, deepfakes, microtargeting—operationalized by platforms and AI toolchains.

Reasoning chain from foundational principles to the specific topic

1. Foundational models quantify how information propagates, aggregates, and is corrupted in networks (information theory, consensus models) [1][2].
2. Abstract social influence models map agent-level updating rules (e.g., weighting, thresholds) onto networked diffusion, showing conditions for rapid belief shifts or robust pluralism.
3. Domain literatures translate these dynamics into institutional practices: states and firms design messaging, channels, and organizational processes to exploit network vulnerabilities and persuasion heuristics.
4. Specific artifacts (robots, synthetic media, recommender systems) operationalize scaling and targeting functions, automating what industrial-era bureaucracies and mass media did manually.

Canonical papers in the foundational layers ground this chain by specifying mathematical conditions for consensus, resilience to adversarial nodes, and network fragility. For example, distributed consensus and adversary-resistant protocols offer formal analogues for defensive information architectures in social systems [1][2]. The conceptual map presented earlier (Conceptual Map: Cognitive Wars) is used to link these layers: foundational primitives -> abstract dynamics -> domain practices -> specific implementations.

Historical Context: Industrialization and Wars

Industrialization changed scale, speed, and social integration: mass production and transport reduced latency in moving troops and materiel, while telegraphy, print runs, radio, and later mass media enabled synchronized narratives across large populations. Mass education and bureaucratization produced standardized cultural referents (national curricula, administrative records) that both enabled mobilization and created centralized targets for cognitive operations. Wars increasingly targeted home fronts: conscription, rationing, morale campaigns, censorship, and propaganda made civilian populations central to strategic outcomes. These developments institutionalized state capacity to project narratives and to collect information, laying the groundwork for modern cognitive warfare.

Mechanisms: Industrialization's Influence on Cognitive Conflict

Mechanism 1 — Mass communication infrastructure

Industrial-era technologies (printing presses, telegraph, radio) expanded reach and reduced latency of messages, enabling synchronization of narratives across geographically dispersed audiences. This increased effective audience size and allowed coordinated campaigns (e.g., war bond drives, morale pushes), establishing playbooks for later media ecosystems.

Mechanism 2 — Bureaucratization and standardized education

Large bureaucracies created routinized channels (registries, schools, civil services) and shared mental models (national myths, civic obligations). These shared referents function as levers for cognitive campaigns—disrupting administrative trust or exploiting school curricula produces outsized social effects.

Mechanism 3 — Industrial organizational forms

Firms and state bureaus instituted repeatable processes for message production, audience segmentation, and distribution logistics. Industrial coordination lowered transaction costs for sustained cognitive operations and supported specialization (propaganda units, censorship bureaus), making influence campaigns continuous, not episodic.

Feedback mechanisms

Success in cognitive campaigns reconfigures incentives: states allocate budgets to propaganda, private firms monetize attention economies, and adversaries learn to imitate tactics. Over repeated cycles, these feedbacks lead to greater automation, refining targeting algorithms and amplifying capacity. In the contemporary AI era, the same feedbacks accelerate capability development: data collection improves models; better models enable more effective campaigns; and strategic success creates more resources for further refinement.

Hypotheses and Theoretical Claims

H1: The deeper the industrialization of society—measured by communication density (channels per capita, message throughput) and bureaucratic capacity (administrative reach, standardized education)—the more central cognitive campaigns become in warfare strategy.

H2: Industrialization moderates the effectiveness of cognitive interventions: highly integrated states achieve greater persuasive control due to leverage over centralized channels, but also face greater systemic vulnerability because saturation and contagion of misinformation can cascade through shared referents.

H3: Technologies and organizational practices associated with industrialization produce structural asymmetries (e.g., centralized vs. polycentric media environments, open vs. closed data regimes) that explain cross-actor variation in cognitive warfare outcomes.

These hypotheses are testable via comparative indicators (literacy rates, media reach, size of civil service) and outcome metrics (opinion change, policy shifts, insurgency recruitment rates).

Methodology and Evidence Strategy

Mixed-methods approach:

- Comparative historical analysis: select conflicts across the industrial spectrum to observe variation in cognitive warfare salience.
- Process tracing: document causal mechanisms in key episodes (e.g., WWI/WWII propaganda campaigns; interwar paramilitary communications; late-20th-century industrial-scale influence operations).
- Quantitative indicators: media penetration (newspapers per capita; radio ownership; internet bandwidth), literacy rates, bureaucratic size (civil servants per capita), and measures of influence campaigns (volume of state broadcasts, bot prevalence).
- Measurement of cognitive effect: public opinion shifts (surveys), institutional change (policy reversals, purges), decision disruption (operational delays, deconfliction failures).

Case selection criteria: compare actors with varying industrial depths and media architectures while holding strategic incentives roughly constant (e.g., same theater of conflict or comparable interstate competition). Process tracing emphasizes mechanism-level evidence (who designed messages, distribution logistics, feedback loops).

Case Studies

Case A — Early industrial era

Analysis focuses on 19th-century conflicts where telegraph and mass print began to coordinate political narratives—showing nascent cognitive operations (war reporting, diplomatic leaks) that shaped international perceptions and domestic mobilization.

Case B — Mass-industrial era

World War I/II: systematic propaganda, rationing, censorship, and home-front mobilization illustrate how mass media and bureaucracy institutionalized cognitive warfare; governments built dedicated propaganda ministries and used emerging communications networks to synchronize domestic behavior.

Case C — Late/post-industrial era

Contemporary hybrid conflicts: platform-mediated disinformation, state-sponsored botnets, and synthetic media leverage industrial legacies (centralized information infrastructures, professionalized media industries) while adding automation and algorithmic amplification, producing new contours of asymmetry and vulnerability.

Each case traces mechanisms (infrastructure, organization, feedback) and evaluates cognitive outcomes using process-tracing evidence and where possible, quantitative indicators.

Applications (Parameterized Vignettes)

Vignette 1 — Disaster response under intermittent communications (civil protection and misinformation)

Scenario parameters: urban population of 2M, primary communication channels: municipal broadcast + social platforms; intermittent connectivity (30% of neighborhoods experience >12-hour blackouts); adversarial actor capable of injecting false evacuation orders and fabricated imagery; AI tools generate credible fake local official messages.

Objectives: ensure safe evacuation, maintain trust in official guidance, minimize casualties.

Operational metrics (parameterized):

- Mean Time to Acknowledge (MTTA) critical false alert: time from adversarial injection to detection and public rebuttal. Baseline (no automated detection): MTTA = 6 hours. With AI-based anomaly detectors + cross-channel verification protocols: MTTA = 45 minutes.
- Failure probability (probability of population following false order): baseline = 0.28; with decentralized multi-source verification + SMS/mesh fallback = 0.08.
- False negative rate for alert suppression (probability legitimate alert suppressed as adversarial): baseline = 0.12; with conservative human-in-loop override = 0.03.

Primary failure modes:

- Channel saturation: adversary floods official channels with false content, overwhelming human moderators and generating plausible noise that delays detection (increasing MTTA).
- Trust erosion: repeated false alerts reduce compliance to legitimate orders, increasing casualties over time (long-term failure mode).
- Fragmented delegation: conflicting private actors (NGOs, municipal agencies) issue divergent guidance, producing paralysis.

Mitigations and tradeoffs:

- Decentralize trusted nodes (local community leaders, certified volunteer nets) to reduce single-point failure; tradeoff: increased coordination overhead and slower centralized control.
- Use conservative human-in-loop thresholds to reduce false positives; tradeoff: slower rebuttal times.

Vignette 2 — Autonomous ISR swarm with contested spectrum (military targeting & cognitive effects)

Scenario parameters: ISR drone swarm (50 units) conducting time-sensitive reconnaissance in contested electromagnetic environment; adversary employs jamming, spoofed feeds, and socio-cognitive operations (leaks amplifying kompromat to friendly public); AI analytic pipeline fuses sensor feeds and generates targeting recommendations.

Objectives: maintain situational awareness, provide reliable targeting recommendations, prevent adversarial manipulation of sensor-derived narratives.

Operational metrics:

- Mean Time To Accurate Fusion (MTTAF): time from sensor acquisition to verified fused product. Nominal (no adversary): MTTAF = 90s. Under jamming/spoofing, without adversary-resistant consensus algorithms: MTTAF = 600s. With adversary-aware fusion and redundancy protocols (Diverse sensors + adversarial filters): MTTAF = 150s [1][2].
- Failure probability (probability of false positive target identification due to spoofing): baseline = 0.07; with adversary-resistant consensus and cross-validation = 0.015.

- Decision disruption probability (probability command delays > T_threshold due to contested feeds): baseline = 0.25; with human-in-loop triage and fallback C2 channels = 0.09.

Primary failure modes:

- Sensor poisoning: adversary injects fabricated sensor payloads or deepfake recon images that pass automated checks.
- Consensus failure: distributed fusion nodes reach inconsistent beliefs due to Byzantine nodes or local spoofing, causing divergent recommendations [1][2].
- Cognitive exploitation of operational outputs: adversary leaks manipulated ISR-derived products to media, influencing home-front political support.

Mitigations:

- Byzantine-resilient consensus algorithms and heterogeneity in sensor modalities reduce poisoning risk [1][2].
- Delegation policy: restrict autonomous target engagement to detections corroborated by at least two orthogonal sensing modalities plus a human authorization for kinetic action.
- Diagnostics: monitor variance across node belief states; trigger human review when divergence exceeds threshold or when anomalous cross-correlation patterns appear.

Discussion

These vignettes illustrate parameterized trade-offs: speed vs. trust, automation vs. resilience, centralization vs. coordination overhead. Metrics (MTTA, MTTAF, failure probability) provide operationally meaningful levers for both research and policy evaluation. Failure modes emphasize that cognitive outcomes emerge from socio-technical interactions—technical defenses must be paired with organizational design and ethical delegation policies.

Limits & Open Questions

This section foregrounds operational assumptions and diagnostics, bounded-rationality, and adversarial communications models as explicit present assumptions. It also identifies open empirical and theoretical questions.

Operational Assumptions & Diagnostics

1) Bounded-rationality assumption

Assumption: human and organizational actors have limited attention, compute, and time; they use heuristics and satisficing rather than globally optimal strategies. This affects both defenders (e.g., moderators, commanders) and adversaries (resource-limited actors optimizing impact).

Concrete triggers (operationalizable):

- Attention overload trigger: when inbound message rate per analyst exceeds X (e.g., 500 items/hour), automatic triage and elevated error risk declared.
- Decision-time trigger: if time-sensitive decisions require more than Y minutes for vetted corroboration (where Y is mission-specific), escalate to conservative default actions.

Delegation policies:

- Conservative automation: allow automated triage and preliminary classification, but require human sign-off for high-consequence outputs (policy: human sign-off threshold tied to potential casualty/strategic cost).
- Escalation ladders: automated systems flag suspicious content for human analysts; if human capacity saturated, fallback to pre-specified safe defaults (e.g., maintain status quo, delay action).

2) Adversarial communications model (present assumption)

Assumption: adversaries are strategic, adaptive, and capable of operating across multiple channels. They deploy signals to exploit known heuristics and structural vulnerabilities in information systems.

Concrete triggers:

- Cross-channel inconsistency trigger: when a message appears across channels with divergent provenance but similar content, raise probability of coordinated adversarial campaign.
- Novel-signal trigger: sudden emergence of high-credibility content sources (e.g., impersonated official accounts) that did not exist previously prompts immediate verification protocols.

Delegation policies:

- Certify-and-verification: primary reliance on cryptographic/source provenance when available; if provenance absent, require corroboration across at least three independent sources before acting on high-consequence information.
- Attribution-light defensive posture: prioritize resilience and continuity of operations over immediate public attribution, to avoid strategic surprise from adversary behavioral shifts.

Presenting these as operational assumptions (not future work) makes explicit the trade-offs enforced by human-in-loop constraints and adversarial adaptation. Diagnostics should be instrumented: monitor message arrival rates, analyst workloads, divergence statistics across fusion nodes, and automated anomaly scores; designate threshold-based policies that automatically change delegation rules under stress.

Open questions and boundaries

- Measurement: how to reliably quantify "cognitive effect" across contexts? Surveys capture short-term opinion shifts but miss latent institutional effects; behavioral and institutional proxies are necessary.
- Attribution: how to attribute cognitive outcomes to specific campaigns when multiple actors and organic diffusion co-occur?
- Scaling defensive norms: how to operationalize decentralization of trusted nodes without fragmenting coordination or enabling malicious local authorities?
- Ethical constraints: what legal and normative limits should constrain state defensive cognitive operations (e.g., counter-messaging that manipulates domestic publics)?

These open questions define a research agenda combining formal modeling, case-based inference, and experimental interventions.

Synthesis

Industrialization created a set of durable socio-technical conditions—high-throughput communication channels, bureaucratic homogenization, and industrial organizational capacity—that reconfigured warfare to include cognitive contests as central strategic domains. Contemporary AI-driven influence operations are a technical intensification of these mechanisms: automation reduces marginal costs, data increases targeting specificity, and platform architectures scale reach. Theoretical grounding in information theory and networked consensus elucidates why certain architectures produce vulnerability (centralized channels, homogenous referents) while others confer resilience (redundant, heterogeneous, locally trusted nodes) [1][2].

From a policy perspective, the synthesis points to two high-level prescriptions: (1) reshape information architectures to reduce single-point cognitive vulnerabilities (decentralize trusted nodes, pluralize verification channels), and (2) pair technical defenses (adversary-resistant consensus algorithms, provenance mechanisms) with organizational reforms that codify human-in-loop delegation under bounded-rationality constraints. Recognizing industrialization as a causal foundation reframes historical interpretation (seeing propaganda and mobilization as structural outcomes, not anomalies) and provides a principled lens for anticipating how AI will re-industrialize influence at lower costs and faster feedback cycles.

Implications for Policy and Future Research

Policy recommendations

- Strengthen information resilience by decentralizing critical communication channels and pluralizing trusted nodes (local civic actors, certified community anchors).
- Invest in adversary-aware technical primitives (provenance, Byzantine-resilient consensus for fused intelligence, provenance metadata) and explicit human-in-loop thresholds tied to mission criticality [1][2].
- Institutionalize norms and legal guardrails to balance defensive cognitive measures with democratic values (transparency, oversight, redress).

Research directions

- Quantify industrialization influence: develop composite indices (communication density, bureaucratic integration) and test correlations with cognitive campaign effectiveness.
- Model socio-technical dynamics: integrate network diffusion models with bounded-rational agents and adversarial optimization to simulate realistic campaign-countermeasure arms races.
- Empirical tests: comparative historical studies and modern experiments (controlled messaging interventions, platform-level red-teaming) to validate mechanisms.

Conclusion

This brief makes a theory-first claim: industrialization is a foundational cause shaping the rise, form, and effectiveness of cognitive wars. The same socio-technical mechanisms that made propaganda and mass mobilization central in the 20th century are being replicated and intensified by AI and platform architectures today. Addressing cognitive wars requires combined technical, organizational, and normative solutions grounded in an understanding of how information propagates, how institutions shape belief systems, and how adversaries exploit structural vulnerabilities.

[1]: On graph theoretic results underlying the analysis of consensus in multi-agent systems. ArXiv.Org (2009).

[2]: Consensus of multi-agent networks in the presence of adversaries using only local information. Dl.Acm.Org (2012).

Assumptions Ledger

Assumption	Rationale	Observable	Trigger	Fallback/Delegation	Scope
Industrialization causally transformed warfare by enabling large-scale cognitive campaigns ("cognitive wars").	Historical evidence links the rise of mass communication, mass education, and centralized administration with deliberate state and non-state propaganda, morale campaigns, and home front targeting; these institutional and material changes plausibly increased reach, synchronization, and the ability to target beliefs at scale.	Historical patterns: growth in circulation and reach of print/telegraph/radio, creation of dedicated propaganda/PSYOP bureaus, archival records of mass mobilization campaigns, measures of public opinion volatility during industrialization-era conflicts.	When mapping causes of large-scale influence campaigns in historical case studies or when assessing whether a society's transformations alter the role of information in conflict.	If the causal link is weak in a given case, treat cognitive campaigns as contingent tactical choices rather than structural outcomes; delegate analysis to case-level social, cultural, and political explanations (e.g., ethnic cleavages, religious mobilization) and incorporate those factors into the model.	Applies to societies undergoing sustained increases in communication throughput, bureaucratic reach, and standardized education; does not claim universality across all pre-industrial or non-state contexts and does not by itself predict specific tactics or effectiveness in every conflict.
Contemporary AI-driven influence operations are an industrialization re-run: automation, datafication, and platform architectures replicate and magnify the mechanisms that made cognitive warfare central in the industrial era.	AI and platforms expand message production, targeting, and distribution capacities while lowering marginal costs, mirroring how printing, telegraphy, and bureaucracies scaled earlier efforts; early empirical work shows automation of amplification and microtargeting	Indicators such as growth in AI-generated content prevalence, automated account networks, increased microtargeted ad spending, platform API features enabling mass personalization, and documented campaigns using AI tools to optimize messaging.	When evaluating modern influence campaigns, assessing risk from new tooling, or projecting trajectories of influence capability as a function of technological adoption.	If AI does not materially magnify mechanisms in a given domain, treat contemporary operations as incremental rather than structural; focus on human organizational drivers (commercial ad markets, political operatives) and on platform governance, and delegate detailed technical assessment to AI system audits and platform telemetry teams.	Applies where digital platforms, large datasets, and AI toolchains are widely accessible; less applicable in low-connectivity environments or where platform governance and regulation strongly constrain automation.

Assumption	Rationale	Observable	Trigger	Fallback/Delegation	Scope
	producing measurable influence effects.				
Bureaucratization and standardized education create shared referents and centralized channels that function as levers for cognitive operations.	Mass schooling and administrative systems produce common knowledge, records, and rituals which both enable coordinated messaging (shared frames) and create high-value targets (registries, curricula) whose disruption or manipulation can yield outsized effects.	Presence of national curricula, centralized civil registries, high literacy rates, uniform media schedules, historical cases where altering curricula or administrative messages produced measurable shifts in public opinion or behavior.	When identifying vulnerable nodes for influence operations, designing defensive resilience (e.g., protecting registries), or assessing which social structures amplify messaging.	If bureaucratization is not a primary lever, shift focus to alternative cultural coordination mechanisms (religious institutions, local elites, kin networks) and delegate intervention design to anthropologists or local governance experts.	Relevant in contexts with significant state administrative reach and standardized public education; less relevant for highly fragmented, low-bureaucracy, or deeply plural societies where shared referents are weak or localized.
Industrial organizational forms (hierarchies, firms, specialized units) enable scalable, repeatable influence operations by lowering transaction costs and supporting specialization.	Organizational theory and historical examples show that firms and bureaucracies create routines, division of labor, and logistics that make continuous campaigns feasible and efficient compared with ad hoc, decentralized efforts.	Existence of permanent propaganda departments, contracted media firms, documented workflows for message production and distribution, budgets for sustained communications campaigns, and evidence of repeated, improved operations over time.	When modeling the persistence and scale of influence operations or when designing countermeasures that target the supply chain of messaging (e.g., disrupting production or distribution pipelines).	If operations are decentralized and not driven by industrial organizational forms, pivot to network-based interventions (e.g., influencer norms, community moderation) and delegate coordination disruptions to platform policy teams and civil-society organizers.	Applies to contexts where formal organizations, markets, or state bureaus coordinate influence work; less applicable to emergent grassroots campaigns or highly decentralized viral phenomena that do not rely on industrial processes.
Feedback loops—where successful cognitive campaigns	Theory and evidence of learning loops show that	Rising budgets and staffing for influence units after successful operations,	When observing repeated success in campaigns, surges in	If feedback loops are weak or broken, prioritize resilience measures (media	Most relevant in settings with available data, funding, and

Assumption	Rationale	Observable	Trigger	Fallback/Delegation	Scope
generate incentives and resources that further optimize influence capabilities—drive accelerating capability, especially in the AI era.	resource allocation follows perceived success; in digital ecosystems, data collected from campaigns trains better models, which in turn improve campaign effectiveness, creating a positive feedback dynamic.	measurable performance improvements over successive campaigns, accumulation of training data tied to operational outputs, and platform-level investments in tooling for targeting and optimization.	funding or talent into influence functions, or rapid improvement in campaign metrics that suggest adaptive learning.	literacy, defensive architectures) and delegate offensive capability analysis to specialized research teams; employ regulatory levers to limit data pipelines and slow feedback acceleration.	institutional incentives to iterate (commercial platforms, well-resourced states or firms); less applicable where data collection is constrained, budgets are static, or institutional learning is slow or absent.

Notation

Symbol	Meaning	Units / Domain
n	number of agents	$\mathbb{N}$
$G_t=(V,E_t)$	time-varying communication/interaction graph	—
$\lambda_2(G)$	algebraic connectivity (Fiedler value)	—
p	mean packet-delivery / link reliability	[0,1]
τ	latency / blackout duration	time
λ	task arrival rate	1/time
e	enforceability / command compliance	[0,1]
τ_{deleg}	delegation threshold	[0,1]
MTTA	mean time-to-assignment/action	time
P_{fail}	deadline-miss probability	[0,1]

Claim-Evidence-Method (CEM) Grid

Claim (C)	Evidence (E)	Method (M)	Status	Risk	TestID
Industrialization increased the centrality of cognitive campaigns in warfare: greater communication density and bureaucratic capacity causally raise the strategic importance of organized influence (H1).	[2] (consensus/adversary multi-agent literature); [3] (historical-political communication studies on propaganda and mass mobilization); [5] (military doctrine/PSYOP describing bureaucratic capacity and centralized messaging).	Comparative-historical empirical analysis linking measures of industrialization (communication channels per capita, registries, literacy rates) to quantitative indicators of cognitive campaign centrality (propaganda budgets, censorship activity, measures of home-front targeting). Complementary regression analysis and synthetic-control counterfactuals; robustness checks with agent-based simulations to test causal mechanisms.	E cited; M pending empirical analysis and simulation (see T1).	If false, the core causal anchor tying industrialization to cognitive-war prominence collapses: theory would need to locate other structural drivers (e.g., ideological, technological, or geopolitical) and reinterpret historical case studies.	T1
Mass communication infrastructure (printing, telegraph, radio; analogously pipelines and platforms) increases effective audience size and reduces message latency, enabling synchronized narratives and scalable campaigns.	[1] (graph-theoretic/consensus primitives relevant to propagation and latency); [3] (historical studies of telegraph/radio effects on wartime coordination); [4] (reports on modern platform amplification and throughput).	Archive-based historical case studies measuring reach and latency before/after introduction of key media technologies; network-diffusion simulations parameterized by measured channel capacities to show effects on synchronization and cascade sizes.	E cited; M pending archival measurement and diffusion simulations (see T2).	If incorrect, the mechanism that links infrastructure to large-scale coordinated influence weakens, undermining claims about why scale and synchronization emerged with industrial media and their digital analogues.	T2
Bureaucratization and standardized education produce shared referents	[5] (doctrinal descriptions of using administrative levers	Mixed-methods: qualitative archival analyses of cases	E cited; M pending case studies and	If wrong, policies that aim to defend or exploit bureaucratic/educational	T3

Claim (C)	Evidence (E)	Method (M)	Status	Risk	TestID
(common frames, records, civic curricula) that function as levers for cognitive operations—attacking or co-opting these referents yields outsized system-level effects.	in PSYOP); [6] (political-psychology evidence on schema, framing, and shared narratives); [3] (sociological history of mass education and state-making).	where administrative systems or curricula were targeted; survey and experimental work testing susceptibility of populations to messages that exploit shared referents; cross-national comparisons linking standardization indices to vulnerability measures.	field/lab experiments (see T3).	leverage points may misfire; the thesis must seek alternative mechanisms for population-level susceptibility to influence.	
Success generates feedback loops (operational success → resource allocation → automation/optimization) that institutionalize and accelerate cognitive-warfare capabilities; contemporary AI-driven influence is an industrialization 're-run' via automation, datafication, and platforms.	[4] (grey/technical reports documenting investment cycles in automated influence and platform monetization); [1] (formal models of iterative adversarial optimization and network effects); [3] (empirical accounts of capability accumulation in state/private actors).	Dynamic-system modeling of investment-feedback loops, agent-based simulations coupling capability growth to effectiveness, longitudinal empirical analysis of funding, personnel, and tool proliferation in state and private actors.	E cited; M pending dynamical modeling and longitudinal empirical validation (see T4).	If false, predictions about exponential capability growth and the analogy between industrial-era institutionalization and modern AI-driven amplification are overstated; countermeasures and policy responses would need recalibration.	T4
Industrial organizational forms (hierarchies, specialized bureaus, repeatable production processes) lower transaction costs and enable sustained, repeatable influence operations—making influence continuous rather than episodic.	[5] (PSYOP and organizational doctrine describing specialized units); [3] (organizational sociology of industrial firms and state bureaus); [6] (evidence on role specialization in communication campaigns).	Organizational case studies, archival process-tracing of bureau/firm formation and routines, comparative institutional analysis; stylized agent-based models to show how specialization affects persistence and scale of campaigns.	E cited; M pending qualitative casework and organizational modelling (see T5).	If wrong, the role of organizational form in sustaining cognitive campaigns is overstated—continuous campaigns may instead arise from other factors (technology, market incentives), affecting mitigation strategies.	T5

Claim (C)	Evidence (E)	Method (M)	Status	Risk	TestID
Foundational consensus and adversary-resistant network models provide useful analytical primitives to model social information propagation and defenses against adversarial nodes; these formal tools can map to social-system interventions.	[1] (graph-theoretic consensus literature); [2] (peer-reviewed work on consensus with adversaries); [6] (political-psychology mappings from micro-updating to aggregate dynamics).	Formal mathematical analysis (proofs) extending consensus/adversary results to social-update rules; numerical simulations of opinion dynamics with realistic heterogeneity and adversarial strategies; validation against empirical diffusion patterns.	E cited; M pending formal extension and simulation-based validation (see T6).	If the formal primitives poorly map onto social systems, model-based predictions (e.g., about resilience, optimal defenses) will be unreliable and could misguide policy interventions.	T6
Automation, datafication, and platform architectures (bots, recommenders, microtargeting) materially amplify diffusion speed and adversarial effects beyond manual industrial-era methods, changing scale and subtlety of influence.	[4] (technical/gray literature on computational propaganda, bots, and recommenders); [3] (peer-reviewed studies quantifying bot amplification and microtargeting effects); [6] (experimental evidence on tailored messaging effects).	Platform-level empirical measurement (traffic, bot prevalence, engagement multipliers), controlled experiments on recommender exposure and tailored messaging, and simulations comparing manual vs. automated campaign trajectories.	E cited; M pending platform measurement and controlled experiments (see T7).	If incorrect, the scale and qualitative novelty attributed to AI/platform-driven influence may be overstated; regulation and defensive design priorities would shift.	T7

Sources

[1]
In 'crisis' we trust? On (un) intentional knowledge distortion and the exigency of terminological clarity in academic and political discourses on Russia's war against ...

Link.Springer.Com, 2023-01-01. (cred: 0.50)

https://link.springer.com/article/10.1057/s41268-023-00313-2

Generated: 2025-11-08T16:22:49.145224 | Word Count: 4928

Research Roadmap

- **Phase 1 (Theory)**: Formalize claims, extend proofs, validate against canonical results
- **Phase 2 (Simulation)**: Implement stress tests, sweep parameter spaces, measure convergence/scaling
- **Phase 3 (Empirical)**: Deploy in controlled environments, collect field data, validate predictions
- **Phase 4 (Integration)**: Operationalize with human-in-loop, adversarial hardening, production deployment

Confidence Methodology: Confidence = 0.3·SourceDiversity + 0.25·AnchorCoverage + 0.25·MethodTransparency + 0.2·ReplicationReadiness, where SourceDiversity reflects unique publishers & types, AnchorCoverage reflects share of primary claims with Type-1 anchors, MethodTransparency reflects CEM completeness & assumptions ledger, and ReplicationReadiness reflects sim plan & datasets/params specified.

Prepared under the STI Research Program — theoretical framework subject to revision as data accumulate.