Narrative Engineering in Intelligence and Geopolitics

Author: Eton Chan

Date: 17 September 2025

Abstract

In the age of proliferating information warfare, influence operations have evolved far beyond the paradigms of twentieth-century propaganda. This academic paper presents an exhaustive, interdisciplinary analysis of "narrative engineering," emphasizing strategic inception-like seeding of narratives that flourish seemingly organically within a target society. Moving sequentially through a robust conceptual framework, psychological and technical mechanisms, geopolitical case studies, advanced attribution methodologies, global policy reviews, and ethical as well as future-oriented considerations, this research elucidates how state and non-state actors weaponize information ecosystems. Special focus is placed on emergent AI-driven tools, open-source intelligence (OSINT), stylometry, and machine learning as defensive and offensive means in these operations. Drawing on a broad base of scholarly and policy literature, the paper concludes with evidence-based recommendations and forecasting for the future of narrative engineering in global intelligence and security.

Introduction

Traditional propaganda, as characterized by overt messaging and easily attributable sources, is rapidly being supplanted by a new generation of influence operations that are both subtler and more sophisticated. These operations—hereafter referred to as "narrative engineering"—seek to plant narrative seeds in ways akin to the concept of "inception" from popular culture, nurturing organic proliferation within the cognitive and social architectures of groups, institutions, and nations. The strategic advantage of such inception-like narrative seeding is clear: narratives appear autochthonous, harnessing the inertia of crowd participation, and become harder to identify, counter, or attribute.

Governments, intelligence agencies, and transnational actors are grappling with this paradigm shift. The rise of powerful generative AI models, the ubiquity of social media, and the breakdown of traditional trust infrastructures have created fertile ground for both malign and beneficial narrative manipulation[1]. At the same time, emergent technical, analytical, and policy frameworks are evolving to detect, counteract, and, ethically, even preempt these operations.

This paper embarks on a comprehensive exploration of narrative engineering in intelligence and geopolitics, with the following aims:

- To establish a detailed conceptual and psychological foundation for understanding narrative engineering and its distinctions from classic propaganda.
- To analyze illustrative geopolitical case studies, ranging from Russian election meddling to China’s Belt and Road Initiative and COVID-19 infodemic management.
- To survey advanced methodologies for detection and attribution, including AI, OSINT, and stylometry.
- To compare global policy responses with respect to efficacy, norms, and ethics.
- To forecast future trends in narrative engineering and information ecosystem manipulation.

Expanded Conceptual Framework

Defining Narrative Engineering

Narrative engineering transcends traditional propaganda by focusing on subtle, systemic interventions designed to alter the cognitive environment over time, rather than seeking immediate attitudinal or behavioral shifts. While propaganda is often characterized by one-way, mass communication and overt calls to action, narrative engineering privileges participatory, networked processes in which target audiences themselves become unwitting amplifiers and even authors of the engineered story.

The term encompasses diverse operations:

1. **Deliberate Narrative Seeding**—Planting foundational messages or symbols so that the wider story may be taken up autonomously by the target population.
2. **Participatory and Networked Persuasion**—Leveraging the participatory nature of digital information environments where targets are active agents in content creation, curation, and dissemination.
3. **Hybrid Cyber-Information Operations**—Integrating cyber, psychological, and computational tools to ensure the cross-platform, cross-domain propagation of narratives.

As articulated by Freistein et al., narrative analysis must occur multimodally and critically, with attention paid to power dynamics, cultural resonance, and the often ambiguous boundaries between benign influence and malign manipulation.

Components of a Narrative Engineering Strategy

A robust conceptual framework, informed by recent research, distinguishes between interdependent components at play in narrative engineering[2]:

- **Narrative Seeds:** The initial elements of the story, framed for psychological resonance and network spread.
- **Channels:** The platforms—social, traditional, or hybrid—through which narratives are introduced and amplified.
- **Cognitive Pathways:** The psychological mechanisms activating emotional investment, identification, or oppositional stance.
- **Ecosystem Dynamics:** The interaction between human agents (influencers, bots, traditional media, civil society) and technological systems (algorithms, recommender systems, generative AI).

The rise of *narrative intelligence*—the ability to map, analyze, and influence how stories propagate across complex networks—is central to contemporary information defense and offense.

Frameworks for Characterizing Influence Operations

Over the past decade, several structured frameworks have emerged to model and analyze influence operations, particularly on social networks. Notable among these are:

- **DISARM Framework:** Developed as a master open-source framework for mapping and countering information operations, DISARM structures campaigns into phases (plan, prepare, execute, assess) and details a taxonomy of tactics and techniques comparable in complexity to the cybersecurity domain[45].

- **BEND, AMITT, and SP!CE:** These frameworks dissect narrative and network maneuvers, enabling both red-team (offensive) and blue-team (defensive) analyses.
- **Online Operations Kill Chain:** Designed to track campaign development across platforms and phases, this model is particularly useful for large-scale takedowns.

The shared emphasis of these frameworks is on a *multistage*, *systematized* understanding of campaigns—beyond the ad hoc or anecdotal. Crucially, influence operations are best conceptualized not as isolated events, but as ongoing system interventions responsive to feedback and counter-response.

Psychological Mechanisms of Narrative Seeding

Narrative Persuasion and Cognitive Vulnerabilities

Narratives profoundly shape perception, emotion, and decision-making. Recent neurocognitive studies underscore that narratives activate the default mode network (DMN) and temporoparietal junction (TPJ) in the human brain, particularly when emotionally charged or suspenseful, fostering attention, arousal, and synchrony among audience members[67].

Key psychological levers include:

- **Transportation:** Deep immersion in a narrative reduces critical resistance and enhances susceptibility to persuasive content[8].
- **Identification:** The more individuals see themselves in a narrative or its characters, the more likely they are to accept attendant meanings or behaviors as their own.
- **Parasocial Relationships:** Viewers form pseudo-social attachments to narrative figures, which can be exploited for persuasive impact.
- **Availability and Affect Heuristics:** Dramatic, vivid, or emotionally negative narratives disproportionately influence risk perceptions and choices.

These mechanisms collectively enable inception-like influence—targets adopt and advocate for narratives as if self-originated, even when externally seeded.

Socio-Cultural Factors and Virality

Narratives are more likely to "go viral" when they synchronize brain responses across populations, exploiting culture-specific heuristics and leveraging collective story archetypes[69]. For instance, Chinese and American subjects respond differently to risk narratives, reflecting deep-seated differences in collective vs. individualistic story structures.

Reconstructive Memory and Narrative Transmission

Narrative fidelity degrades or mutates as stories traverse social transmission chains. Cognitive science research identifies *schematic transmission* (retaining basic structure) and *paraphrastic transmission* (rephrasing, adaptation) as the dominant modes, with paraphrastic strategies more prone to distortion and thus to manipulation[7].

Technical Mechanisms of Narrative Seeding

Coordinated Inauthentic Behavior and Algorithmic Manipulation

The core technical enablers of modern influence operations include:

- **Coordinated Inauthentic Behavior (CIB):** The orchestration of networks of accounts (bots, sockpuppets, trolls) to manufacture the appearance of organic grassroots movement or consensus[1011].
- **Algorithmic Amplification:** Manipulation of recommendation and trending algorithms through artificial engagement, keyword and hashtag engineering.

- **Bot Farms and Synthetic Agents:** Increasingly sophisticated use of AI-driven bots, blending real and synthetic activity, often leveraging cheap labor and hardware to create near-undetectable presence[10].
- **Cross-Platform Laundering:** Transferring narratives across platforms and languages to obscure origins and exploit differing local trust contexts.

Generative AI and Deepfakes

In 2024-2025, the explosion of generative AI led to a new wave of highly realistic deepfakes, AI-generated text, and personalized narrative targeting at unprecedented scale. These tools facilitate narrative insertion across modalities—text, image, video, and voice—blurring the lines between fact and fiction and reducing the friction for malicious actors.

AI-driven content has also been shown to exploit Jungian archetypes and cultural signifiers more effectively than previous tech, enhancing emotional resonance and activism potential[913].

Cyber-Enabled Hybrid Operations

Narrative engineering frequently pairs with cyber operations—such as hacking, malvertising, or doxxing—to manufacture "evidence," create information voids, and amplify disruption (for instance, using a deepfake video seeded via a malicious ad campaign).

Case Studies with Geopolitical and Psychological Analysis

Russian 2016 Election Interference

Russia's multi-pronged interference campaign in the 2016 U.S. election exemplifies advanced narrative engineering:

- **Narrative Seeding and Amplification:** Russia's Internet Research Agency (IRA) flooded social media with divisive content, using both true and misleading material to exacerbate existing cultural and political fissures. While "fake news" captured headlines, much of the most effective content was not demonstrably false but strategically framed to resonate with target audiences' preexisting beliefs[1516].
- **Influencer Cascades:** Russian operations actively sought to enlist influential domestic voices—celebrities, activists, politicians—to "launder" narratives into mainstream discourse[1716].
- **Tactical Flexibility:** Strategies included both "direct influence" (pushing new or extreme content) and "consonance" (aligning with and amplifying native grievances).
- **Participatory Propaganda:** A participatory model (as opposed to broadcast/outbound propaganda) was key, with citizens engaging, sharing, and adapting content, often unwittingly.

Analyses indicate these campaigns were often more impactful in polarizing populations and undermining institutional trust than in changing explicit voting behavior. Subtle narrative positioning and marathon repetition—rather than bald lies—were central to this outcome.

Chinese Belt and Road Initiative (BRI)

China's BRI illustrates the use of infrastructural, economic, and cultural narratives on the global stage:

- **Soft Power and Branding:** BRI is not just a set of projects, but a global narrative framing China as the benign architect of shared prosperity. This is reinforced domestically and internationally via official discourse, cultural exchanges, and co-branded institutions (e.g., Confucius Institutes, Silk Road festivals)[18].
- **Symbolic Economy:** Symbolic policy, such as emphasizing China's role as global connector or referencing ancient Silk Road myths, is crucial. Economic projects serve as stage sets for narrative construction.
- **Narrative Contestation:** Western actors counter-narrate BRI as neo-colonial or "debt-trap" diplomacy, creating a contested narrative space that shifts with local, national, and global agendas.[19]

The BRI case demonstrates how narrative engineering is inseparable from concrete policy and infrastructure, and highlights the adaptive, multi-scalar nature of narrative contests.

COVID-19 Infodemic and Vaccine Narratives

COVID-19 presented fertile ground for narrative warfare:

- **Infodemic Dynamics:** Vaccine hesitancy, conspiracy theories, and counterfactual public health narratives spread explosively, exploiting information overload, emotional uncertainty, and lack of trusted messengers[202122].
- **Intervention Varieties:** Governments and international organizations trialed a range of narrative interventions, from fact-checking to gamified inoculation against misinformation to narrative-based corrections.

- **Censorship and Secrecy:** Heavy use of censorship and labeling by platforms/governments caused secondary harms—distrust in authorities, social polarization, and self-silencing of heterodox knowledge[20].

Psychologically, emotionally engaging, identity-relevant narratives resisted countervailing facts. Trusted local messengers (community/religious leaders, healthcare professionals) proved far more effective than impersonal campaigns, echoing findings in political and security studies.

Advanced Detection and Attribution Methodologies

AI and Machine Learning for Detection

Since 2023, a surge of AI-powered detection tools has transformed how influence operations are tracked and attributed:

- **Content and Pattern Analysis:** Transformer-based models (e.g., mBERT, XLM-RoBERTa, RemBERT) are benchmarked for multilingual detection of disinformation patterns and linguistic anomalies[24].
- **NLP Sentiment and Topic Analysis:** Advanced NLP pipelines analyze lexical, semantic, and sentiment patterns to flag inauthentic content, emotional manipulation, and echo-chamber formation[9].

While AI outpaces humans in speed and scalability, it remains challenged by adversarial adaptation, "hallucination," and overreliance on pattern recognition (risking false positives, especially with satire or culturally specific storytelling)[252112].

Open Source Intelligence (OSINT)

The maturation of OSINT—now AI-augmented—has been integral for both detection and attribution:

- **Automated Social Media and Web Monitoring:** Tools such as Maltego, Shodan, SpiderFoot, and dedicated narrative intelligence platforms fuse surface/deep/dark web data, enabling entity and network mapping at scale[263].
- **Visual and Trend Analysis:** AI-powered image/video analysis and real-time trend prediction have become vital for tracking viral narratives, especially those spread via deepfakes or image memes.
- **Workflow Best Practices:** Multi-stage workflows are advised—combining rapid, broad detection with granular, human-in-the-loop source verification and context assessment[263].

Stylometry and Machine Learning-Based Authorship Attribution

Stylometry—the computational study of linguistic style—has advanced through the application of machine learning and neural networks:

- **Function Words and N-Grams:** Analysis of commonly used function words (and now, multi-layered n-gram networks) reliably identifies unique authorial fingerprints, even across translation and paraphrasing attempts[2728].
- **Cluster-Based Attribution:** Unsupervised and supervised stylometric models can now cluster document authorship, trace temporal style changes, and link multi-author texts within narrative campaigns[2928].
- **Parallel Architecture Approaches:** Combining multiple stylometric features (lemma, PoS, word adjacency, n-grams) with deep learning yields superior attribution accuracy across languages and content types[28].

Case studies demonstrate stylometry's utility in identifying both human and AI-generated content originators, although "style transfer" and adversarial rephrasing remain partial obstacles.

Measuring Impact and Effectiveness of Narrative Operations

Frameworks for Measurement

Measuring the impact of narrative operations is notoriously difficult. Recent frameworks emphasize:

- **Multi-Level Indicators:** Tracking message and messenger reach, audience engagement, shifts in beliefs, and downstream behavioral/cultural/institutional change[30][31][32].
- **Baseline and Context Assessment:** Establishing pre-intervention baselines and continually documenting evolving socio-political contexts.
- **Contribution vs. Attribution:** Emphasis on contribution—linking activities and observed change—rather than seeking definitive attribution for complex, dynamic phenomena[30][32].
- **Four-Part Models:** As detailed by the Stanford Social Innovation Review and Narrative Initiative, impact assessment should consider: creation, translation, driving, and observation of narrative interventions, tracking change in language, story, frame, and social behavior/structure[31][32].

Real-World Application

In recent years, organizations such as EU DisinfoLab have piloted response-impact frameworks to evaluate the cost-effectiveness and downstream consequences (intended and unintended) of counter-narrative operations, factoring in disruption, attribution, deterrence, community mobilization, and resilience building[33].

Empirically, the most successful measurement regimes combine quantitative (views, engagement, sentiment) with qualitative (community trust, resilience, partnership) and policy (regulation, platform practices, legal action) indicators.

Comparative Review of Global Policy Responses

United States

The U.S. has oscillated between limited regulatory intervention (platform self-governance, First Amendment constraints) and more assertive multi-agency efforts. Recent years saw greater coordination between platforms and government in identifying, labeling, and removing coordinated inauthentic behavior networks. However, revelations of covert U.S. PSYOP and influence campaigns have prompted renewed calls for ethical oversight and transparency[34].

Key characteristics:

- **Emphasis on Resilience:** Priority on digital literacy and rapid incident response, as reflected in CISA's TRUST model and best practice advisories[35].
- **Tension Between Free Speech and Security:** Deep-seated legal and cultural reluctance to empower government regulation over narrative content, with ongoing debate about platform responsibility[2523].

European Union

The EU has emerged as a global leader in regulatory, collaborative, and capacity-building responses:

- **Regulatory Frameworks:** The Digital Services Act and the Strengthened Code of Practice on Disinformation demand greater platform accountability, algorithmic transparency, and EU-wide rapid alert systems[36].
- **Institutional Capacity:** Bodies such as the East StratCom Taskforce, the European Centre of Excellence for Countering Hybrid Threats, and the European Digital Media Observatory coordinate cross-border monitoring and rapid response initiatives.

- **Multi-Sectoral Partnerships:** Emphasis on civil society partnership, media plurality, and fact-checker empowerment.

China and Russia

Both Russia and China continue to integrate narrative engineering as a central pillar of their information and political strategies:

- **Russia:** Relies on persistent hybrid warfare, integrating cyber operations, CIB, and tailored narrative interventions across traditional and nontraditional channels, including Telegram and distributed botnets[11517].
- **China:** Deploys unified narratives domestically (Great Firewall) and globally, leveraging economic statecraft (BRI) and cultural/soft power to entrench preferred realities and marginalize dissent or contestation[18].

Global Trend: Policy Gaps and Fragmentation

- **Fragmented Enforcement and Attribution:** International collaboration is hamstrung by varying legal regimes, attribution challenges, and geostrategic competition.
- **Slow Institutional Adaptation:** While platforms and governments have improved at takedown and labeling, adversaries adapt rapidly, exploiting regulatory and technological loopholes.

Ethical Implications of Counter-Influence Strategies

The Moral Authority Dilemma

Counter-influence operations, particularly those involving deception, concealment, or manipulation, risk undermining the moral authority of democratic actors—even as they pursue legitimate defensive aims[37]. Bjola argues that to preserve legitimacy, defenders must commit to:

- **Truthfulness, Prudence, and Accountability:** Clearly demonstrating the nature and scope of their responses, and accepting oversight.
- **Proportionality:** Matching response intensity to actual threats and risks.
- **Transparency and Responsibility:** Avoiding measures that would violate core values or set dangerous precedents for abuse.

The Governance and Oversight Challenge

- **Oversight Failures:** Recent Pentagon PSYOP scandals illustrate failures of contractor oversight and raise debate regarding rules, transparency, and congressional review[34].
- **Risks of Domestic Trust Erosion:** Excessive censorship, covert campaigns, or participation in mass deception—even for defense—may foster cynicism, accelerate polarization, and undercut social trust.

AI Ethics and Human Accountability

The integration of generative AI introduces new risks including:

- **Bias and Opaqueness:** AI algorithms may inadvertently perpetuate systemic biases or make non-transparent decisions.

- **Attribution Ambiguity:** As AI-generated narratives become less distinguishable from human content, assigning responsibility becomes urgent—especially where malicious behavior or error leads to real-world harm.
- **Consent and Civilian Protections:** Blurring lines between military and civilian spheres, especially when defense includes mass participatory disinformation, raises grave ethical questions about protection and consent[4].

The Future of Narrative Engineering

Technological Drivers

- **AI Arms Race:** As bot platforms, deepfake generators, and automated narrative engines proliferate, both adversaries and defenders will increasingly rely on AI "agents"—defensive and offensive—fighting for narrative supremacy in real-time, multimodal, multilingual contexts[112].
- **Hybrid Human-AI Coevolution:** Sophisticated attacks and countermeasures will be increasingly hybrid, with humans and AI systems co-designing, co-monitoring, and co-evolving strategies and defenses.

Operational and Policy Trends

- **Source-Centric Intelligence:** Counter-influence efforts will shift to mapping and monitoring narrative ecosystems using source-centric approaches, filtering by credibility, authority, and network position over brute quantity[3].
- **Global Regulatory Convergence?:** While path-dependency remains, the threat landscape may drive a convergence toward baseline regulatory standards and collaborative incident response structures. The EU, in particular, is expected to remain a pace-setter.

- **Resilient, Participatory Defenses:** Building "cognitive resilience" at the individual and community levels—via critical media literacy, trust networks, and civic engagement—will be as critical as any technical solution.

The "Narrative Integrity" Imperative

Just as cyber hygiene is now a baseline expectation, "narrative hygiene"—the collective ability to recognize, question, and validate stories—must become central to civil society, core institutions, and individual practice. Creativity, critical thinking, and ethical reflection will remain as necessary as any technological advance.

Conclusion

Narrative engineering represents both a peril and an imperative for the twenty-first century security environment. Its power lies in the ability to plant seeds—ideas, story fragments, symbols—that blossom as if native within target information ecosystems, eluding simple detection, countering, and attribution. As demonstrated by the chronicled case studies and the latest research, the frontier of influence is no longer limited to overt propaganda but envelops the entire social-cognitive and technological spectrum.

To defend open societies and their institutions—without sacrificing the very foundations of trust, accountability, and liberty—they must not only detect and counteract malign narrative operations, but also invest in the capacity for adaptive, ethical, and forward-looking narrative stewardship.

The future of geopolitics and intelligence will not merely be a battle of opposing messages, but a contest for the information environments within which our shared realities are imagined, contested, and ultimately, lived.

References

This section includes all sources referenced in-text and is formatted in APA style as per academic standards. Please refer to the "References" section in the downloadable PDF version for full citations.

1*Deepfakes, Bots, and Manipulated Media: The Top Narrative Attacks of ….*
https://blackbird.ai/blog/narrative-attacks-2024-deepfakes-bots-manipulated-media/

2*CHAPTER CONCEPTUAL FRAMEWORKS IN RESEARCH distribute*.
https://us.sagepub.com/sites/default/files/upm-assets/110533_book_item_110533.pdf

3*Proven OSINT Strategies to Enhance Decision Making*.
https://edgetheory.com/products/narrative-intelligence-features/osint-intelligence

4*DISARM Foundation*. https://www.disarm.foundation/

5*DISARM Framework – "Mendeleev's table" of information operations and ….*
https://project-athena.eu/disarm-framework-mendeleevs-table-of-information-operations-and-campaigns/

6*Neural Processing of Narratives: From Individual Processing to Viral ….*
https://www.frontiersin.org/journals/human-neuroscience/articles/10.3389/fnhum.2020.00253/full

7*The Neurocognitive Mechanisms Underlying Narrative Schematic and ….*
https://www.biorxiv.org/content/10.1101/2025.03.13.643115v1.full.pdf

8*The psychological mechanisms of persuasive impact from narrative ….*
https://www.hope.uzh.ch/scoms/article/download/j.scoms.2017.02.003/688/

9*AI Narrative Modeling: How Machines' Intelligence Reproduces ... - MDPI*.
https://www.mdpi.com/2078-2489/16/4/319

10*Bot farms invade social media to hijack popular sentiment*.

https://www.fastcompany.com/91321143/bot-farms-social-media-manipulation

11*Modeling the Impact of Social Media Bots for Information Dissemination*.

https://www.cmu.edu/ideas-social-cybersecurity/events/2024_ideas_cmot_lynnette.pdf

12*Confronting AI-based Narrative Manipulation in 2025: Top Tech ....*

https://blackbird.ai/blog/confronting-ai-narrative-manipulation/

13*The Future of Storytelling: Using Generative AI and Prompt Engineering ....*

https://larrycollett.com/the-future-of-storytelling-using-generative-ai-and-prompt-engineering-to-innovate-content-creation/

14*Received: Applying the DISARM Accepted: Framework to a Cognitive ....*

https://www.acigjournal.com/pdf-190196-112700?filename=Cyber Influence Defense_.pdf

15*Here's What We Know So Far About Russia's 2016 Meddling - TIME*.

https://time.com/5565991/russia-influence-2016-election/

16*Russian Information Operations: Strategies and Tactics of Influence*.

https://netsysci.cut.ac.cy/wp-content/uploads/2019/09/JensenEtAl_Russia_infoOps2016_APSA2019.pdf

17*Leaks, Lies, and Altered Tape: Russia's Maturing Information ....*

https://securingdemocracy.gmfus.org/russias-maturing-information-manipulation-playbook/

18*The Belt And Road Initiative: Shaping The Narrative Of A China Story ....*

https://fpa.org/the-belt-and-road-initiative-shaping-the-narrative-of-a-china-story/

19*Wind of change: shifting narratives on China's Belt and Road Initiative ....*

https://academic.oup.com/cjres/article/18/2/403/8140592

20*A Narrative Review of the COVID-19 Infodemic and Censorship in ….*

https://researchandappliedmedicine.com/revistas/vol2/revista3/a-narrative-review-of-the-covid-19-infodemic-and-censorship-in-healthcare-doi-8.pdf

21*Frontiers | Unravelling the infodemic: a systematic review of ….*

https://www.frontiersin.org/journals/communication/articles/10.3389/fcomm.2025.1560936/full

22*Infodemic Management Approaches Leading up to, During, and Following ….*

https://centerforhealthsecurity.org/sites/default/files/2023-04/230407-nasempaper.pdf

23*Countering Disinformation Effectively: An Evidence-Based Policy Guide ….*

https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide?lang=en

24*[2509.10737] PolyTruth: Multilingual Disinformation Detection using ….*

https://arxiv.org/abs/2509.10737

25*AI and Misinformation: How to Combat False Content in 2025*.

https://business.columbia.edu/insights/magazine/ai-and-misinformation-how-combat-false-content-2025

26*15 Best OSINT Tools of 2025 : Unleash Your Inner Detective*.

https://technicalustad.com/best-osint-tools/

27*Authorship attribution in translated texts: a ... - ACL Anthology*.

https://aclanthology.org/2024.propor-2.15.pdf

28*Parallel Stylometric Document Embeddings with Deep Learning Based ….*

https://www.mdpi.com/2227-7390/10/5/838

29*[2401.06752] Stylometry Analysis of Multi-authored Documents for ….*

https://arxiv.org/abs/2401.06752

30*A Four-Part Framework for Measuring Narrative Change*.

https://ssir.org/articles/entry/four-part-framework-measuring-narrative-change

31*Measuring Narrative Change - ORS Impact*.

https://www.orsimpact.com/DirectoryAttachments/7182019_123705_659_Measuring_narrative_Change_FINAL_rev_17July2019.pdf

32*How to Measure Narrative Change - The Commons*.

https://commonslibrary.org/how-to-measure-narrative-change-2/

33*Beyond Disinformation Countermeasures: Building a Response-Impact ….*

https://www.disinfo.eu/publications/beyond-disinformation-countermeasures-building-a-response-impact-framework/

34*Pentagon PSYOP Scandal Demands an Urgent Debate on Propaganda Ethics*.

https://www.techpolicy.press/pentagon-psyop-scandal-demands-an-urgent-debate-on-propaganda-ethics/

35*Preparing for and Mitigating Foreign Influence Operations Targeting ….*

https://www.cisa.gov/sites/default/files/2023-01/cisa_insight_mitigating_foreign_influence_508.pdf

36*EU Code of Practice on Disinformation | European Commission*.

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/strengthened-eu-code-practice-disinformation_en

37*The Ethics of Countering Digital Propaganda | Ethics &amp ….*

https://www.cambridge.org/core/journals/ethics-and-international-affairs/article/abs/ethics-of-countering-digital-propaganda/DF393C0793F31EE0940E9208E24CB6A8