

Seeding Perceptions: Modern Influence Operations in Global Security

Author: Eton Chan

Date: 9/24/2025

Introduction

The landscape of global security in the twenty-first century is increasingly defined by the contest over perceptions, narratives, and beliefs. While the instruments of hard power military force, economic leverage, political coercion remain vital, the ability to shape opinion, sow discord, and manipulate truths has emerged as an indispensable tool for both state and non-state actors. This research report seeks to dissect the multidimensional phenomenon of modern influence operations: the orchestration of disinformation campaigns, psychological operations, and strategic narratives across social, digital, and traditional channels. These operations transcend ideological confines; they permeate democracies and autocracies, exploit partisan divides, and operate in theaters as diverse as the Middle East's sectarian tapestry, the digital public squares of the West, and the evolving power geometries of the Global South.

This study unfolds in three movements. First, it interrogates the theoretical underpinnings and historical evolution of influence operations. Second, it surveys contemporary practice through in depth case studies, drawing on recent empirical evidence from Russia, China, the United States, Iran, Israel, European powers, and non-state actors. Finally, it explores the technological, psychological, and sociopolitical mechanisms that both enable and constrain modern influence campaigns, uncovering underexamined linkages and emergent threats particularly in the age of artificial intelligence, information laundering, and transnational narrative warfare.

Throughout, the focus is global and interconnected. To advance new insights, this report rigorously connects timelines, mechanisms, and outcomes correlating influence operations with observable shifts in public opinion, policy formation, or escalatory spirals in conflict. The

research synthesizes dozens of international and regional sources, primary documentation, expert analysis, and state of the art fieldwork. The result is a comprehensive, systems level survey designed to inform practitioners, scholars, and policymakers navigating an era where the battle for truth is, increasingly, a battle for security itself.

Theoretical Foundations of Influence Operations

Defining Influence Operations

At its core, an influence operation is a coordinated, targeted activity often clandestine that seeks to alter attitudes, behaviors, or perceptions of individuals, groups, or entire societies in a way that advances the interests of the initiating actor, usually at the expense of an adversary. The U.S. RAND Corporation defines influence operations as the “coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster attitudes, behaviors, or decisions by foreign target audiences that further national interests and objectives”¹².

The term encompasses a spectrum of activities:

- Disinformation (deliberate spread of false or misleading content)
- Misinformation (unintentional spread of inaccurate information)
- Psychological operations (PSYOP) aimed at shaping cognition and morale
- Strategic communications (stratcom) for agenda setting and agenda framing
- Reflexive control (manipulation of adversary decision making)
- Digital and hybrid tactics involving bots, AI, and information laundering

A significant challenge in the academic literature and among practitioners is the lack of clear and uniform conceptual boundaries between “information operations,” “strategic communication,” “psychological warfare,” and “influence operations,” all of which sometimes overlap in real world execution.

The Historical Evolution: From Propaganda to Reflexive Control

While propaganda and psychological manipulation are as old as politics itself evident in Sun Tzu's teachings and the "fog of war" described by Clausewitz as the codification of influence operations accelerated in the twentieth century. World War I and II saw the institutionalization of psychological operations in military doctrine and statecraft. Propaganda ministries, radio broadcasts (e.g., BBC, Voice of America, Radio Free Europe), and leaflet drops over battlefields set early precedents.

The Cold War redefined the field. Both the West and the Soviet bloc considered "information warfare" essential to ideological competition, regime survival, and the orchestration of so called "active measures", a Soviet term that captured a host of covert activities, from forgeries and rumors to black propaganda and front organizations⁴⁵.

The theory of "reflexive control," originating in Soviet military thought, posits that by proactively shaping an adversary's perceptions, a state could indirectly compel irrational or self-defeating decisions on the opponent's part of a framework still prominent in contemporary Russian doctrine. Reflexive control is uniquely powerful because it seeks not just to inform or mislead, but to act on the logic and mental models through which decisions are made.

Influence in the Digital Age: Models and Frameworks

The explosion of digital connectivity and social media transformed the scale, speed, and character of influence operations. New models emerged:

- The "firehose of falsehood," a term coined by RAND, to describe campaigns (notably Russia's) that prioritize volume, speed, and repetition across multiple channels, regardless of internal consistency or objective truth, exploiting the psychological phenomena whereby repeated statements and apparent consensus increase perceived credibility⁷⁸.
- The Diamond Model for Influence Operations, which integrates socio-political axes (influencer and audience) with technical axes (capabilities and infrastructure) centered on narrative as the core variable.
- The DISARM and SP!CE frameworks, developed to map the phases, tactics, and techniques of online social network influence campaigns, supporting the analysis of "cyber kill chains" and indicators of compromise.

Crucially, as observed by the U.S. Army War College and the GAO, contemporary influence operations blend technical sophistication (AI driven bots, deepfakes, social network microtargeting) with social engineering and the exploitation of psychological vulnerabilities(see also).

Historical Evolution of State Sponsored Psychological Operations

Psychological Operations in the Cold War

The Cold War institutionalized psychological operations (PsyOps) at an industrial scale⁹⁴. The United States and Soviet Union both developed dedicated bureaucracies in the U.S. Army's Psychological Operations Group (5th PSYOP), KGB "active measures" units, and the British Information Research Department focused on shaping the "hearts and minds" of both domestic and foreign audiences.

The period was characterized by:

- The use of "white," "gray," and "black" psyops ranging from overt, attributed communications to wholly covert or deceptive campaigns.
- Coordinated media manipulation, exemplified by the alleged U.S. Operation Mockingbird, in which major news outlets and journalists were recruited or influenced to promote narratives aligned with U.S. foreign policy interests, both domestically and internationally¹⁰¹¹.
- The propagation of disinformation campaigns like the Soviet "Operation INFEKTION," which sought to blame the U.S. for the origin of HIV/AIDS, or the manipulation of the "Red Scare" in the West for internal political purposes.

These operations were more than isolated incidents: they reflected evolving doctrine. For the United States, "winning the war of ideas" accompanied, and sometimes supplanted, traditional hard power.

Post-Cold War Adaptation

As the Cold War ended, the logic of psyops did not disappear but was reconfigured. The focus shifted to “human terrain operations,” the attempt to shape decision making among military adversaries, civilian populations, and political elites in asymmetrical or hybrid wars¹. The Gulf Wars, interventions in the Balkans, Afghanistan, and Iraq, and the responses to terrorism post 9/11 all saw psyops adapted to new theaters: from leaflet drops to digital “hearts and minds” campaigns in local dialects, to leveraging satellite television and nascent internet channels. Parallel to military doctrine was the rise of “public diplomacy” and “strategic communication” as tools for agenda setting both at home and abroad.

Russian Influence Operations: Mechanisms, Timelines, and Effects

The Russian Doctrine: From “Active Measures” to the “Firehose of Falsehood”

Russian influence operations, steeped in Soviet tradition, have evolved into one of the most sophisticated and global campaigns in the modern era. Russian doctrine treats information and perception management as a decisive strategic domain. As one recent U.S. Army War College report noted, “Russia generally controls perceptions among targeted audiences to shape the environment to its benefit... [and] few emphasize information operations on par with Russia”¹².

Key features of Russian modern influence operations include:

Hybrid Warfare: Russia’s 2016 definition frames hybrid warfare as “a strategic level effort to shape the governance and geostrategic orientation of a target state, in which all actions, up to and including the use of military force, are subordinate to an information campaign”⁶.

Reflexive Control: Manipulating information environments to prompt adversaries to choose courses of action deemed favorable to Russian interests, often by masking or distorting true risks and rewards.

Firehose of Falsehood: High volume, multichannel dissemination of contradictory, rapid, and repeated messages with no commitment to objective reality or internal consistency; experimental

evidence suggests the sheer volume and repetition imparts familiarity and greater acceptance, even of patently false claims⁷⁸.

Information Laundering: Transposing false or fringe narratives into the mainstream by rebroadcasting across layers of more reputable channels and proxy websites, a process witnessed in the spread of conspiracy stories about U.S. biolabs in Ukraine or “bio weaponized birds” in recent European theaters¹³.

Infrastructure and Methods

The Russian information apparatus spans state channels (RT, Sputnik), semi official “troll farms,” and a vast web of proxy outlets, as well as armies of bot driven accounts and sock puppets operating across all major global platforms. Russian narratives are tailored for domestic, regional, and international audiences, often with varying degrees of subtlety (e.g., more crude, demotic propaganda for domestic consumption; subtler, more reasoned narratives for Western liberals)⁶.

Table: Key Mechanisms of Russian Influence Operations

Mechanism	Description	Target/Channel
State Media (RT, Sputnik)	Official, multilingual news output; quasi-journalism	Domestic, international (TV, web, social)
Proxy Websites, Alt-Media	Hidden ownership, often “alternative” branding	Blogs, YouTube, local news outlets
“Troll Farms”	Paid operators creating fake personas, sowing discord	Social media (Twitter/X, Facebook, Instagram)
Automated Bots	Algorithmically managed accounts amplifying narratives	All social platforms
Think Tanks/NGOs Fronts	Nominally “independent,” amplifying Kremlin lines	Policy and academic circles
Information Laundering	Layering of dubious stories through multiple outlets	News cycle, social media, political debate

The resilience and redundancy of the network make counteraction difficult: even as platforms ban known assets, new accounts and proxy sites emerge.

Contemporary Case Studies

Georgia (2008) and Crimea (2014): Russian operations included manufactured media events, orchestrated confusion over “green men” (unmarked soldiers), and the rapid deployment of contradictory narratives about Ukrainian culpability in violence, with Western and local news outlets at times amplifying unfounded claims.

Ukraine War (2022-25): Investigations revealed near real-time duplication of Kremlin originated narratives across international media, with the deliberate use of “bio-weaponized birds” and similar stories to delegitimize U.S. policy and portray Ukrainian leadership as unstable or criminal. The goal: exploit partisanship in Western democracies and erode trust in institutions¹².

Western Elections (2016-present): Russian linked networks, including DC Weekly and others, have faked U.S. news personas and sowed disinformation (e.g., fake Black Lives Matter protests, false stories targeting immigrant communities, and antivaccine conspiracies), materially influencing political discourse and trust in electoral outcomes¹².

Correlation with Policy and Opinion Shifts

Post 2014, Russian disinformation campaigns in Europe and the U.S. broadly contributed to the intensification of political polarization, declining trust in institutions, and in some Central and Eastern European states measurable shifts in attitudes toward NATO and the European Union¹². Surveys in Slovakia and Hungary reveal a post 2022 uptick in public belief in “Western aggression” and skepticism of Ukraine narratives, influenced by a media ecosystem penetrated by Russian and pro Kremlin proxies¹².

Evidence demonstrates that the impact of influence operations is greatest in environments marked by:

- Media fragmentation
- Low trust in traditional news
- “Echo chambers” structured along ideological, linguistic, or ethnic lines

Chinese Strategic Media Influence and Global South Narratives

Chinese Information Strategy: Creating an “Alternative Order”

China’s approach to influence operations is both distinct and increasingly assertive. Unlike Russia’s chaos driven “firehose” model, the Chinese Communist Party (CCP) leverages a coherent, top down narrative project: offering the Global South a vision of international order as a counterpoint to U.S. led liberal hegemony¹⁴.

Key elements of Chinese influence operations include:

State Media and Managed Diplomacy: Xinhua, China Global Television Network (CGTN), and affiliated outlets push China’s benign, development focused narrative while selectively amplifying Western missteps and instability. During forums such as the Xiangshan Forum, an “alternative platform” to the Western led Shangri-La Dialogue, China hosted over 1,800 representatives from 100 countries, shaping security discourses with a focus on “multilateralism,” “historical truth,” and “anti-hegemonic resistance”¹⁴.

Narrative Reinterpretation: Chinese speakers at these forums link modern grievances (e.g., Taiwan, South China Sea) with historical struggles (e.g., resistance to colonialism) framing Chinese policies as restoration rather than revisionism, legitimacy rather than aggression¹⁵.

Global South Targeting: China targets states like Brazil, Nigeria, India, and Vietnam with tailored communications asserting China as an “honest broker” representative of “true multilateralism,” creating alternatives to U.S.-centric institutions. The launch of the Global Governance Initiative (GGI) and related strategic and economic frameworks at back to back summits reinforces China’s claim to being a champion of non Western voices¹⁵.

Antagonistic Media Events: State media capitalize on confrontations (for example, a public dispute between a Chinese academic and an Israeli officer over the Gaza war) to push anti-Western or anti-Israel narratives, establishing China as a moral voice supporting the Muslim world and the Global South¹⁶.

Technical Integration: Digital Censorship and External Propaganda

China's model is unique in its combination of internal digital censorship ("Great Firewall," AI driven monitoring, and content removal) and expansive external propaganda, now leveraging generative AI for external narrative laundering¹³.

The use of synthetic personas, deepfakes, and AI generated news articles allows Chinese state narratives to be laundered through foreign social networks and third party outlets obfuscating their origin and enhancing credibility in the local context. Recent Graphika and State Department reports document widespread use of fake personas (e.g., the fictitious columnist "Yi Fan" disseminating CCP talking points worldwide) and laundering of state media content across multiple social platforms¹³.

The synergy between China and Russia is crucial. Both powers now coordinate, at least tacitly, on international narratives (e.g., "hegemonic bullying" by the West, the legitimacy of alternative security forums), with China increasingly exploiting Russia's dependence for its own agenda¹⁷¹⁸.

Influence Outcomes in the Global South

In Africa and Latin America, China's narrative has demonstrably shifted local discourses about development, governance, and the balance of international legitimacy¹⁵. Engagements like the Belt and Road Initiative, digitally amplified, have led some analysts to describe the rise of a "parallel information order", where states or populations disillusioned with the West's reliability look to Beijing for partnership and ideological validation.

Yet Chinese efforts are not without friction. The preference for direct, transactional relationships over multilateral, genuine partnership, and the uneven results of "soft power" campaigns in key countries continue to limit global narrative dominance¹⁴.

United States Influence Campaigns: Legacies and the Digital Pivot

Historical Paradigms: From Operation Mockingbird to Public Diplomacy

The U.S. has been both a target and prolific practitioner of influence operations. Early paradigms like the CIA's purported Operation Mockingbird saw prominent American journalists and editors acting as assets or informants, shaping narratives for both foreign and, allegedly, domestic audiences during the Cold War¹⁰¹¹. While the details and extent are contested, Congressional inquiries confirmed at least dozens of confirmed relationships between the CIA and major U.S. news outlets during the 1950s-70s.

Beyond covert media placement, U.S. psychological operations included overt broadcasts (Voice of America, Radio Free Europe), cultural diplomacy (student exchanges, support to foreign print media), and “black” or “gray” propaganda campaigns. U.S. doctrine also involved the use of strategic communication in pro-democracy movements and, later, in counterterrorism narratives throughout the post 9/11 period¹⁹.

Contemporary U.S. Efforts: Counter-Disinformation and Strategic Narratives

In the twenty-first century, the U.S. emphasis shifted toward countering adversary disinformation (notably Russia, China, Iran, and non-state actors), with efforts coordinated by the Department of State's Global Engagement Center, Department of Homeland Security, and Department of Defense Public Affairs.

Key methods include:

Public Exposure and Fact Checking: Publishing detailed threat reports, collaborating with platforms, and debunking major disinformation stories (e.g., about election interference, vaccine misinformation, and foreign influence).

Education and Resilience Building: Promoting media literacy and critical thinking in U.S. and allied populations, often through partnerships with NGOs and local governments²⁰.

“Influencer Briefings” and Social Media Campaigns: Working with digital creators, especially on TikTok, YouTube, and Instagram, to proactively disseminate U.S. foreign policy explanations and counter adversary narratives. In the context of the Ukraine war, credentialing

hundreds of influencers for political conventions and organizing private briefings with White House staff demonstrate the increasing integration of digital native actors into U.S. influence campaigns.

Digital Strategy and the Challenges of Defending Open Systems

Despite these efforts, the open information environment in the U.S. and many Western democracies remain vulnerable to manipulation. The incentives for social media companies maximizing engagement rather than accuracy or truthfulness and the speed of viral misinformation present structural obstacles to counter disinformation efforts²⁰.

Recent U.S. reviews and Congressional investigations highlight persistent coordination gaps across government agencies, ongoing debates over First Amendment boundaries, and insufficient capacity for rapid, large-scale debunking or inoculation against sophisticated digital influence attacks²⁰.

Iran's Proxy Networks and Regional Influence Operations

The Iranian Model: Revolutionary Export Through Proxy Forces

Iran's model of influence is rooted in the ideology of its 1979 revolution and the doctrine of "exporting the revolution." The Iranian Revolutionary Guard Corps (IRGC), and specifically its Quds Force, orchestrates a network of allied militant groups and social movements across the region from Hezbollah in Lebanon and Shia militias in Iraq, to the Houthis in Yemen and various Palestinian factions²¹²².

Key characteristics:

Ideological and Pragmatic Blending: Iranian foreign policy combines hardline Shi'a Islamism (vilayat-e faqih, anti-Zionism, anti-Americanism, pan-Islamism) with pragmatic country and context specific alliances including with Sunni actors like Hamas when interests align²².

Proxy Warfare: Through the IRGC-QF, Iran trains, funds, and equips non-state actors, enabling Tehran to project power while maintaining plausible deniability and avoiding direct confrontation. This network, sometimes described as the “Shia Crescent,” encompasses thousands of armed operatives across Iraq, Syria, Lebanon, Yemen, and, to a much lesser degree, the Palestinian Territories²³.

Table: Timeline of Key Iranian Proxy Developments

Year/Period	Event/Development
1979-1989	IRGC and Quds Force established; opening to external proxies
1982	Creation/support of Hezbollah in Lebanon
1990s	Support for Palestinian (Sunni) groups and emerging alliances
2003-2011	U.S. invasion of Iraq creates opening for Shia militia networks
2014-2019	ISIS threat catalyzes PMF (Hashd al-Sha'abi) and expands Syrian engagement
2015-2024	JCPOA, regional expansion, and direct confrontations with Israel/U.S.
2020-2025	Intensified Houthi attacks in Yemen, multi-front support to groups in Israel-Gaza crisis

Influence Mechanisms and Effects

Operational Flexibility: Iran adapts its networks, providing cash, advanced weaponry (missiles, drones), or logistical support as required, while allowing proxies substantial autonomy at tactical levels²¹.

Media and Information: Iran and its proxies operate local and global media arms (e.g., Al-Manar, PressTV, online propaganda channels), blending parochial sectarian narratives with broader anti-Western, anti-Israeli, and anti-Saudi themes²².

Impact: Iranian proxy actions like rocket attacks, cyber operations, logistical corridors from Iran to Lebanon have contributed to shifts in regional power balances. Notably, the rise of the PMF in Iraq reoriented Iraqi politics, while Hezbollah's entrenchment in Lebanese politics, and the Houthis' regional reach, have constrained rival actors and placed persistent pressure on Israel and U.S. allies²¹²².

Israel's Strategic Narratives and Hasbara in Regional Conflicts

Evolution of "Hasbara" and the Strategic Narrative Campaign

Israeli public diplomacy ("hasbara") exemplifies a hybrid model blending state directed and civil society driven influence operations. The objective is both to explain (and thus justify) Israeli actions to international audiences and to counter perceived delegitimization efforts, especially in times of conflict²⁴²⁵.

Key mechanisms:

State Infrastructure: The IDF Spokesperson's Unit, Ministry of Foreign Affairs, and Prime Minister's Office coordinate official messaging. Since 2017, the Israeli government has prioritized digital platforms operating across 30+ social media platforms, sponsoring hundreds of paid campaigns annually, and employing professional "public diplomacy specialists" whose roles now go beyond foreign embassies into real-time engagement with global audiences²⁴²⁵.

Civil Society and "Volunteer War Rooms": In every major round of conflict (e.g., 2023-25 Gaza crisis), hundreds of volunteer organizations, tech companies, and individuals coordinate

operations to produce, disseminate, and amplify content globally. This bottom-up phenomenon has powerful multiplicative effects, especially in English speaking and Western social media ecosystems²⁴.

Tactical Adaptivity: Israeli campaigns exploit paid advertising, emotionally resonant content, influencer partnerships (including with conservative U.S. and European social media figures), and rapid responses to incidents (e.g., the al-Ahli Hospital bombing, countering Hamas narratives in under 24 hours using detailed forensic evidence and direct interventions from Israeli civil and state actors). Campaigns also target international institutions, such as UN bodies and NGOs, with paid advertisements and coordinated social media countercampaigns²⁵.

Outcomes and Domestic Constraints

While Israeli hasbara efforts maintain significant influence, particularly in the United States and parts of Europe, they face persistent challenges: negative perceptions in parts of the Global South, accusations of emotional manipulation or disinformation, and increasing global scrutiny of the use of paid influence, especially when state narratives conflict with widely reported humanitarian crises (e.g., alleged famine in Gaza)²⁵.

The evolution reflects both technical sophistication mass data driven advertising buys, microtargeted content, AI powered operations and vulnerabilities characteristic of democratic information environments: volunteer fatigue, declining impact in adversarial or undecided audiences, and backlash to overtly defensive or heavily managed messaging²⁵.

European Union and National Counter-Disinformation Frameworks

EU-Wide Approaches and Policy Instruments

Since 2016, the European Union has recognized disinformation as a major threat to open society, trust in institutions, and democratic resilience²⁶³²⁰.

Core elements:

Code of Conduct and Digital Services Act (DSA): The Code of Practice on Disinformation (2018, revised 2022, integrated into the DSA in 2025) creates an enforceable framework for “Very Large Online Platforms” (e.g., Meta, Google, TikTok) to demonstrate auditable compliance on measures including demonetization of disinformation, transparency in political advertising, algorithmic labeling of misleading content, and improved access to data for vetted researchers²⁶²⁷.

Platform Driven and Civil Society Partnerships: The EDMO (European Digital Media Observatory) and DisinfoLab coordinate research, fact checking, and cross border threat intelligence sharing. Member states maintain dedicated national strategies ranging from criminalization to large scale media literacy investments and regulatory frameworks focused on content moderation by private “information intermediaries” (e.g., platforms and ad networks)²⁷. A pluralistic, “multi-stakeholder” approach combines soft measures (education, fact checking) with more stringent regulatory and legal regimes. Major member states like Germany (NetzDG), France (Loi Avia), and the Nordics have pioneered approaches integrating platform liability and accountability for information disorder; however, implementation and results remain uneven²⁷.

Impact and Challenges

Reviewing the effectiveness of these frameworks, the EDMO finds uneven, often superficial compliance by major platforms, ongoing opacity in data access for researchers, and persistent gaps in real world accountability²⁷. The policy debate in Europe increasingly focuses on moving from “reactive” to “proactive” content moderation, developing systematic (algorithmic or human) interventions, and improving coordination in the face of rapidly evolving, AI enabled threats(see also²⁰).

Technology of Influence: Bots, Avatars, and AI Driven Campaigns

Automation and the New Digital Battleground

Since the 2010s, influence operations have exploited the scalability of automated technologies: botnets, AI avatars, microtargeted advertising, and now generative AI, all allow a handful of actors to propagate massive volumes of content, manipulate trending topics, and generate the illusion of grassroots consensus or outrage²⁸²⁹.

Bots and Sock Puppets: AI controlled or human managed avatars can flood social platforms, manipulate conversations, or send encoded signals through covert “community” management a tactic now sophisticated enough to use encrypted overlays, shifting network topologies, and deniable encryption (Community Covert Communication Technique-CCCT) to evade even the most advanced detection systems.

AI Avatars and Virtual Influencers: AI generated personas (virtual influencers) are overtaking traditional digital celebrities, able to create emotionally resonant, tailored content at scale. Avatars can communicate in dozens of languages, bypass content moderation, and create lifelike video, audio, and text, opening new vectors for persuasive manipulation or coordinated inauthentic behavior²⁹.

Table: Automation in Digital Influence Campaigns

Technology	Function	Example Use Case
Botnets	Mass amplify messages, trend hijacking	Election “astroturfing”
AI Avatars	Lifelike digital influencers, microtargeting	International marketing and politics
Deepfakes	Synthetic media, impersonation	Political scandal, discreditation
CCCT/CCC	Encrypted covert communication	Espionage, intelligence transfer

Chatbots	Automated persuasion, sentiment shaping	Voter outreach, propaganda relays
----------	---	-----------------------------------

Opportunities and Threats in Governance

While these technologies offer efficiencies in marketing and information dissemination, they also present unprecedented challenges:

- Difficulty in attributing actors
- Rapid obsolescence of detection/defense tools (AI outpaces content moderation)
- Vulnerability to “information laundering” (where synthetic or obscure narratives can be layered through semi-credible proxies into mainstream discourse)³¹

The feedback loop of AI generated disinformation and algorithmic amplification is now recognized by both government and academic researchers as a critical threat to cognitive security, requiring new regulatory, technical, and societal responses²⁰.

Non-State Actors: Terrorist and Extremist Influence Tactics

Case Study: ISIS and Online Radicalization

The Islamic State (ISIS/ISIL), al-Qaeda, and other jihadist organizations have pioneered the use of modern media, social networks, and encrypted platforms for influence operations, focusing on both recruitment and the intimidation of adversaries³²³³.

- **Multi-Platform Propaganda:** ISIS utilized Twitter, YouTube, Telegram, encrypted chatrooms, and bespoke apps to disseminate ideological videos, operational instructions, and martyrdom tales. Social media campaigns used hashtags, memes, and viral tactics modeled on commercial marketing³²³³.
- **Hybrid Messaging:** Research indicates that the most effective radicalization messages downplay graphic violence, instead emphasizing the material, spiritual, and social benefits of joining jihad; powerful imagery of brotherhood, prosperity, and shared purpose drove online

engagement far more than beheading videos, which appealed mainly to hardened extremists³².

Adapting to Enforcement and Expanding Reach

As mainstream platforms increased enforcement, ISIS and affiliates adapted, relying on ever smaller, encrypted channels (e.g., Telegram), developing dark web platforms, and shifting to decentralized peer to peer models. Meme culture blending far-right online aesthetics with jihadist content is now recognizable (“Alt-Jihad” subcultures on TikTok and Instagram)³³.

Regional and Localized Influence

ISIS’s recruitment strategies in sub-Saharan Africa, West Africa, and the Sahel region are rooted in local grievances, inequality, neglect, and state abuses layered over global jihadist narratives. Group media wings both produce localized, vernacular content and contribute to the ISIS international propaganda ecosystem (Amaq News Agency, Mujahideen TV, etc.)³³.

Underexplored Mechanisms: Information Laundering and Reflexive Control

Information Laundering: The Digital “Clean-Up” of Disinformation

Information laundering describes the process by which misleading or fabricated content is propagated through networks of dubious, semi-credible, and ultimately mainstream outlets, acquiring legitimacy along the way in the same way illicit funds acquire the trappings of legality³¹.

Key stages:

- Placement on obscure sites, fringe blogs, fake personas, or state sponsored “news” portals
- Layering through higher credibility intermediaries (think tank reports, social media influencers, alternative news channels)

- Integration into global or national media discourse, frequently after key attribution data has been stripped away (“source laundering”)

Nation states including Russia and China, terror networks, domestic extremists, and even commercial interests have all employed information laundering to influence public debate and create synthetic consensus or controversy (e.g., conspiracies about COVID-19, 5G, and “biolabs”)³¹.

Technological advances, generative AI, deepfakes, mass automated content translation escalate the challenge, enabling the rapid localization and topical laundering of global disinformation at a scale outpacing most current detection frameworks.

Reflexive Control in Practice

The concept of reflexive control, prompting adversaries to adopt self-defeating actions by shaping their perception space remains a central pillar of advanced Russian influence doctrine⁶. Wittingly or unwittingly, targeted societies can be maneuvered into polarizing disputes, overreactions, or “decision paralysis,” as seen in debates over freedom of expression, pandemic response, or migration crises.

Correlations Between Influence Campaigns and Sociopolitical Shifts

Global North: Case Analyses

Rigorous analysis correlates the rise of targeted influence operations with measurable increases in political polarization, erosion of trust in democratic institutions, and public misperception concerning policy areas like migration, health, and crime²⁰¹².

In the United States, intensification of Russian linked “fake news” and disinformation campaigns in the run-up to the 2016 and 2020 presidential elections correlated with spike in anti-institutional sentiment, belief in conspiracies, and willingness to doubt electoral legitimacy effects mirrored, with variations, in the context of Brexit and recent European elections³²⁰.

Table: Summary of Opinion/Policy Shifts Linked to Influence Operations

Region/Country	Campaigns/Mechanisms	Measured Effects
U.S./UK/EU	Russian, Chinese, domestic alt-media, “firehose” campaigns	Increased polarization; distrust in media, elections, science
Latin America	WhatsApp/zero-rated “fake news” (e.g., Brazil 2018)	Electoral upsets, swift swings in political narratives
Nigeria, Africa	Youth voter mobilization, misinformation on WhatsApp	Volatile political participation, propaganda-driven unrest
Middle East	Iran proxy/militia info war, Israeli hasbara, U.S. PSYOP	Shifts in legitimacy, public protest participation, security calculus

Global South: Patterns and Impact

The digital transformation of political communication in emerging democracies exposes new vulnerabilities. In Brazil (2018), the combination of messaging app networks, business elites, and “zero rated” platforms enabled the spread of viral fake news directly undermining center left candidates. In Nigeria, the 2023 election cycle saw political influencers on TikTok, WhatsApp propaganda, and AI driven voter manipulation, with empirical studies documenting both enhanced engagement and new waves of strategic polarization³⁴³⁵.

More broadly, limited digital literacy, asymmetric platform access, and the economic structure of data in the Global South intensify the influence of digital operations and complicate mitigation efforts.

Comparative Analysis of Major Actors' Influence Strategies

Actor/Region	Strategic Objective	Primary Mechanism	Key Innovations	Notable Outcomes
Russia	Disrupt, sow discord in West	Firehose of falsehood, proxies, reflexive control	Automation, information laundering	Election interference, polarization, policy paralysis
China	Promote alternative order, defend sovereignty	Strategic narrative, "forum shopping," AI-generated outreach	Managed diplomacy, external AI avatars	Growing Global South alignment, narrative soft power
United States	Defend order, promote democracy	Public diplomacy, fact-checking, influencer engagement	Digital education, influencer integration	Inconsistent resilience, evolving platform engagement
Iran	Regional power via proxies	Proxy networks, asymmetrical alliances, ideological narrative	Localized hybrid tactics, deniability	Reshaped regional alliances, enabled low-cost escalation
Israel	Defend legitimacy, secure support	Hasbara/public diplomacy, civil activism, paid social	Mass digital ad buys, rapid narrative response	Sustained Western support, contentious global debate

EU and Members	Defend democracy, build resilience	Regulatory (DSA, Codes), education, research alliances	Multistakeholder compliance, standardized indicators	Enhanced platform accountability, uneven application
Non-State Actors	Recruitment, intimidation	Social media campaigns, encrypted comms, hybrid narrative	Alt-jihad, decentralized online subculture	Persistent global radicalization, lone-wolf attacks

Global South Case Studies: Latin America, Africa, Southeast Asia

Brazil

The 2018 presidential election in Brazil marked a watershed in information manipulation. WhatsApp, enabled by “zero rating” plans restricting the broader internet but providing free access to Facebook and WhatsApp, became the conduit for daily viral misinformation targeting candidate reputations and policies. Business lobbies funded illegitimate campaign contributions for “fake news” spread, driving polarization and undermining faith in electoral institutions. The dynamic reflects a broader pattern in Latin America where digital platforms outpace regulatory and civil society responses³⁶.

Nigeria

Nigeria’s 2023 elections illustrate how social media, particularly WhatsApp, Twitter/X, TikTok, and Instagram, have supplanted traditional rallies as the dominant arena for political contest. Influencers drive youth engagement, and WhatsApp groups enable rapid mobilization, even as misinformation, fabricated endorsements, and AI generated content vastly outstrip verification capabilities. While digital activism increased overall participation, empirical research confirms that misinformation facilitated new forms of polarization, confusion, and periodic disengagement among key demographics³⁵.

In Indonesia, the 2019 presidential election evidenced the incursion of “Russian-style” disinformation into local campaigns; memes, fake news, and framing tactics contributed to the deepening of ethnic, religious, and ideological divides. Facebook’s “Free Basics” offering and platform centric internet limited public exposure to reliable, alternative sources, furthering the efficiency of propaganda and viral content lacking critical scrutiny³⁶.

Conclusion: New Patterns, Persistent Challenges, and Strategic Implications

Modern influence operations have evolved into a complex, systematized phenomenon that transcends ideological, regional, and technological boundaries. The case studies and mechanisms surveyed in this report reveal several emergent patterns:

Hybridization and Adaptive Learning: State and non-state actors dynamically borrow from each other, blending kinetic, psychological, social, and digital tools to maximize impact.

Influence operations are no longer the exclusive province of intelligence agencies, they mobilize volunteers, privatized firms, AI driven avatars, and local proxies in intricate feedback loops.

Automation and AI as Force Multipliers: The democratization and mass adoption of generative AI, deepfakes, and automated influence engines have dramatically increased the efficiency, velocity, and targeting capability of modern operations. As both attackers and defenders harness AI, the battle for digital truth becomes a contest of speed, reach, and machine powered adaptation.

Information Laundering and Narrative Layering: Increasingly, the path from fringe theory to mainstream belief passes through layered laundering mechanisms. This development raises urgent challenges for traditional fact checking, journalism, and regulation, as attribution and provenance become harder to establish.

Cognitive Security as the New Front Line: The psychological resilience of populations in their media literacy, capacity to distinguish credible from incredible, and resistance to both subtle and overt manipulation is now as critical to national security as military hardware or diplomatic alliances.

Global South as the Testing Ground: Emerging democracies and developing countries, with differential access to digital literacy and information, are laboratories for new influence techniques often with the greatest impact on participation, polarization, and democratic stability. Bridging the gap between exposure and resilience demands a new strategic paradigm, one that recognizes the multidimensional nature of contemporary information warfare, harmonizes regulatory regimes across borders, and centers the empowerment of citizens as the final defense. As the dynamics of influence operations continue to shift, so too must the understanding and response of those tasked with defending open societies. The war for perceptions is now as consequential as the war for territory, and the outcomes for policy, peace, and the persistence of truth itself are still unfolding.

References (42)

1. RAND Corporation. (n.d.). *Foundations of effective influence operations: A framework for enhancing Army capabilities*. Retrieved from <https://www.rand.org>
2. Santa Maria, S. D. (n.d.). *Improving influence operations by defining influence and influence operations*. Retrieved from <https://apps.dtic.mil>
3. Recorded Future. (n.d.). *The diamond model for influence operations analysis*. Retrieved from <https://go.recordedfuture.com>
4. Broda, E., & Strömbäck, J. (n.d.). *Misinformation, disinformation, and fake news: Lessons from an interdisciplinary, systematic literature review*. Retrieved from <https://academic.oup.com>
5. History Rise. (n.d.). *Psychological warfare in the Cold War: Propaganda and paranoia shaping global tensions*. Retrieved from <https://historyrise.com>

6. Military Dispatches. (n.d.). *The role of PsyOps in the Cold War: Strategies and impact*. Retrieved from <https://militarydispatches.com>
7. Army History. (n.d.). *Cold War weekend warriors: The 5th Psychological Operations Group*. Retrieved from <https://armyhistory.org>
8. RAND Corporation. (n.d.). *The Russian “firehose of falsehood” propaganda model*. Retrieved from <https://www.rand.org>
9. Wikipedia contributors. (n.d.). *Firehose of falsehood*. Retrieved from <https://en.wikipedia.org>
10. VSquare. (n.d.). *Firehose of falsehood*. Retrieved from <https://vsquare.org>
11. Wikipedia contributors. (n.d.). *Operation Mockingbird*. Retrieved from <https://en.wikipedia.org>
12. All That’s Interesting. (n.d.). *Operation Mockingbird: The CIA’s plan to control the media*. Retrieved from <https://allthatsinteresting.com>
13. Vault Terminal. (n.d.). *Operation Mockingbird: Examination of media influence strategies*. Retrieved from <https://vaultterminal.com>
14. Foreign Policy Research Institute. (n.d.). *The fight against disinformation: A persistent challenge for democracy*. Retrieved from <https://www.fpri.org>
15. Wikipedia contributors. (n.d.). *Information laundering*. Retrieved from <https://en.wikipedia.org>
16. The Diplomat. (2025). *Xiangshan Forum: China enters a new era of assertive global influence*. Retrieved from <https://thediplomat.com>
17. Raisina Hills. (n.d.). *Xiangshan Forum: Beijing’s counterweight to the West*. Retrieved from <https://theraisinahills.com>

18. Udumbara. (n.d.). *Chinese state media capitalize on confrontation at forum to push anti-West narrative*. Retrieved from <https://udumbara.net>
19. Royal United Services Institute. (n.d.). *Russia and China: The true nature of their cooperation*. Retrieved from <https://www.rusi.org>
20. CNA. (n.d.). *Russia and China have drawn closer: Three ways to wedge them apart*. Retrieved from <https://www.cna.org>
21. Springer. (n.d.). *Russia-China relations: Emerging alliance or eternal rivals?*. Retrieved from <https://link.springer.com>
22. Carnegie Endowment for International Peace. (n.d.). *Countering disinformation effectively: An evidence-based policy guide*. Retrieved from <https://carnegieendowment.org>
23. Nature. (n.d.). *Misinformation poses a bigger threat to democracy than you think*. Retrieved from <https://www.nature.com>
24. SSRG International Journals. (n.d.). *Iran's proxy strategy: Militant networks and regional influence*. Retrieved from <https://www.internationaljournalsssrg.org>
25. Center for Strategic and International Studies. (n.d.). *War by proxy: Iran's growing footprint in the Middle East*. Retrieved from <https://www.csis.org>
26. Frontline (The Hindu). (n.d.). *How Iran's Islamic Revolutionary Guard Corps, its Quds Force operate*. Retrieved from <https://frontline.thehindu.com>
27. Wikipedia contributors. (n.d.). *Hasbara*. Retrieved from <https://en.wikipedia.org>
28. Institute for National Security Studies. (n.d.). *Civil public diplomacy (Hasbara) in the Gaza War*. Retrieved from <https://www.inss.org.il>

29. EBU Spotlight. (n.d.). *Inside Israel's digital Hasbara offensive*. Retrieved from <https://spotlight.ebu.ch>
30. European Commission. (n.d.). *The Code of Conduct on Disinformation*. Retrieved from <https://digital-strategy.ec.europa.eu>
31. DisinfoCode. (n.d.). *Code of Conduct on Disinformation*. Retrieved from <https://disinfocode.eu>
32. European Digital Media Observatory. (n.d.). *Implementing the EU Code of Practice on Disinformation: An evaluation*. Retrieved from <https://edmo.eu>
33. DISA. (n.d.). *Automated avatars used in covert social media influence operations*. Retrieved from <https://disa.org>
34. Analytics Insight. (n.d.). *From code to fame: How AI avatars are taking over social media*. Retrieved from <https://www.analyticsinsight.net>
35. AI Model Agency. (n.d.). *The rise of AI avatars: Transforming social media interaction*. Retrieved from <https://aimodelagency.com>
36. Homeland Security Affairs Journal. (n.d.). *Fake news, conspiracy theories, and lies: An information laundering perspective*. Retrieved from <https://www.hsaj.org>
37. Wikipedia contributors. (n.d.). *Social media use by the Islamic State*. Retrieved from <https://en.wikipedia.org>
38. Columbia Magazine. (n.d.). *How ISIS really recruits its members*. Retrieved from <https://magazine.columbia.edu>
39. Small Wars Journal. (n.d.). *ISIS's transition and the interplay of online and face-to-face recruitment*. Retrieved from <https://smallwarsjournal.com>

40. The Conversation. (n.d.). *WhatsApp skewed Brazilian election, showing social media's danger to democracy*. Retrieved from <https://theconversation.com>
41. NaijaSpider. (n.d.). *How social media will influence the 2027 Nigerian elections*. Retrieved from <https://blog.naijaspider.com>
42. IIARD Journals. (n.d.). *Impact of media on the citizenry during political campaigns in Nigeria*. Retrieved from <https://iiardjournals.org>