

Overwatch

BY MIAMI STRATEGIC INTELLIGENCE INSTITUTE



Miami Strategic
Intelligence Institute

SIGNATURE ESSAY

THE ENEMY DOES NOT NEED TO BREAK IN

How Russia, China, Iran, and Their Proxies Recruit Open Societies Against Themselves

By Dr. Rafael Marrero

MSI² President, Founder, and CEO

The most dangerous foreign asset may be the citizen who never realizes he
has been recruited.

BOTTOM LINE UP FRONT

MSI² assesses (High Confidence): Russia, China, and Iran do not need to persuade a majority of Americans or Latin Americans to adopt an authoritarian worldview. They need only to identify authentic grievances, conceal the foreign hand, borrow trusted local voices, and convert outrage into paralysis, polarization, economic dependency, or policy advantage. Russia favors disruption and distrust. China more often pairs narrative management with trade, technology, infrastructure, and elite access. Iran fuses ideological messaging with cyber-enabled influence and a Spanish-language echo chamber supported by aligned regional media. Digital amplification and human cultivation are complementary: money, ideology, compromise, and ego can move a useful voice toward access, dependency, and deliberate tasking. Their methods differ, but their operational opportunity is the same: the openness, speed, and commercial incentives of democratic information systems. The answer is not censorship. It is attribution, transparency, resilience, strategic economic engagement, and a citizenry trained to ask who benefits before it shares.

WHY THIS MATTERS

Influence operations target the decisions that precede formal power: what voters believe, what journalists normalize, what universities excuse, what investors finance, what governments procure, and which foreign partners a society comes to regard as inevitable. Once narrative capture makes an adversary's presence appear natural, market access, diplomatic leverage, sanctions erosion, and strategic infrastructure can follow at a fraction of the cost of coercion.

A fictional scene with a real warning

In the Paramount+ series *Lioness*, the episode titled "The Idiot Army" pauses the gunfire long enough to expose a quieter battlefield. The threat is not an invading formation. It is a hidden network moving through respectable professions, ordinary relationships, and familiar channels of trust. The drama compresses a complex national-security problem into a brutal idea: an adversary can build strategic power inside a free society without placing every participant on a payroll or giving every participant an order (Paramount+, 2026).

The phrase "useful idiots" is often attributed to V. I. Lenin, including in the episode. The attribution is not substantiated. William Safire's search of Lenin's published work, assisted by the Library of Congress, found no documentary basis for it, and later quotation research reached the same conclusion (Boller & George, 1989; Safire, 1987; Shapiro, 2019). The correction matters. A serious essay about manipulated belief should not open with a doubtful quotation.

However, the warning survives the bad attribution. The core problem is not low intelligence. It is strategic utility. Highly educated people can be more useful than the gullible because they possess status, language, networks, and institutional access. They can translate a foreign narrative into the moral vocabulary of their own society. They can make it sound native. They can turn propaganda into commentary, commentary into consensus, and consensus into policy.

The danger, however, is also easy to abuse. A citizen who opposes a war, criticizes Washington, questions a trade policy, protests for Palestinian rights, defends engagement with China, or doubts a sanctions regime is not thereby a foreign instrument. Democracies are supposed to contain hard disagreement. The evidentiary line is not whether a view helps an adversary. It is whether the activity involves concealed sponsorship, deceptive identity, coordinated direction, coercion, criminality, or a knowing effort to disguise provenance. Canada's foreign-interference inquiry drew the same distinction: diplomacy and even aggressive persuasion can be legitimate when open, whereas interference becomes malign when covert, deceptive, or threatening (Public Inquiry into Foreign Interference, 2025).

Five categories democracy must not confuse

Category	What the evidence must show
Witting agent	Knows the foreign sponsor or tasking and acts on its behalf.
Proxy or intermediary	May know the direction or benefit, but obscures the chain between sponsor and audience.
Access agent or facilitator	Opens doors, supplies introductions, or lends legitimacy. The role may be witting or unwitting, so direction and intent still require evidence.

Category	What the evidence must show
Unwitting amplifier	Repeats, localizes, or legitimizes a narrative without knowing its origin or strategic purpose.
Independent dissenter	Exercises protected speech without covert foreign direction, deception, or coercion.

This discipline protects both national security and civil liberty. If every dissenter becomes a suspect, the adversary wins twice: first by manipulating debate, then by provoking the democracy into discrediting its own principles.

From useful voice to controlled asset: MICE, honeypots, and the recruitment threshold

Recruitment rarely announces itself. It may begin with a flattering invitation, a conference dinner, a business introduction, a private message after a television appearance, or someone who seems unusually interested in a person's frustrations. The first request is often harmless. The danger lies in the second, the third, and the tenth, when favors become expectations and an ordinary relationship begins to move beyond its boundaries.

Counterintelligence professionals have long used MICE as shorthand for four pressures that can turn access into dependence. Money can arrive as cash, consulting fees, gifts, debt relief, travel, contracts, or business opportunities. Ideology can be political, religious, nationalist, or rooted in a sincere belief that the targeted country has betrayed its own values. Compromise or coercion can involve secrets, illicit conduct, threats to family or reputation, or emotionally intimate material that creates leverage. Ego is the warmest door: flattery, status, exclusivity, recognition, academic degrees, resentment, and the intoxicating sense of finally being treated as important (Burkett, 2013; Canadian Security Intelligence Service, 2021).

A honeypot belongs inside that framework, but it should not swallow the essay. It is the cultivation of a target through romantic, sexual, or emotionally intimate access to obtain information, influence behavior, create dependency, or generate compromising material. In practice, intimacy may serve ego, enable compromise, or do both. Official Canadian guidance warns that foreign actors can build deep, even romantic relationships over time, while UK guidance cautions that hostile states use deceptive online identities to approach people with access to valuable information, places, or networks (Canadian Security Intelligence Service, 2021; National Protective Security Authority, 2025).

The movement from useful voice to controlled asset is therefore a continuum, not a label. An unwitting amplifier advances a narrative without understanding its origin or strategic purpose. An access agent opens doors, offers introductions, or confers legitimacy. A recruited asset knowingly accepts direction or tasking. A honeypot target is being cultivated through intimacy. The defensive question is not who someone dated, befriended, or met abroad. It is whether the record shows concealed sponsorship, deception, coercion, escalating dependency, knowing service, or repeated boundary crossings.

THE LINE THAT MATTERS

A honeypot is a method, not a verdict. An affair, friendship, foreign contact, or controversial belief is not proof of recruitment. The evidentiary threshold remains concealed sponsorship, deception, coercion, tasking, or knowing service to a foreign interest.

How the story enters the bloodstream

Influence operations rarely begin with a wholly fabricated grievance. They begin with something true enough to hurt: corruption, inequality, a civilian casualty, a closed factory, an arrogant official, a failed project, or a forgotten community. The operator then supplies a story that converts pain into certainty. One villain explains everything. One institution is irredeemable. One foreign power is blameless. Compromise becomes betrayal.

That is why narrative is the weapon system. Research on narrative transportation shows that a coherent story can absorb attention, emotion, and imagination in ways that shape story-consistent beliefs (Green & Brock, 2000). Studies of online diffusion find that moral-emotional language increases sharing within ideological networks, while false news in the studied Twitter dataset traveled farther and faster than accurate news (Brady et al., 2017; Vosoughi et al., 2018). The adversary does not need a perfect lie. It needs an emotionally efficient explanation delivered by someone the audience already trusts.

The MSI² influence conversion chain

1. **Find the fracture.** Map a genuine grievance, identity conflict, policy failure, or economic anxiety.
2. **Frame the grievance.** Replace complexity with a morally absolute story that rewards anger and punishes doubt.
3. **Borrow the messenger.** Use local journalists, commentators, academics, activists, business leaders, community organizations, or synthetic personas.
4. **Launder the source.** Translate, edit, repost, quote, and cross-cite until the foreign origin disappears and repetition resembles corroboration.
5. **Convert attention into advantage.** Depress trust, fracture alliances, weaken sanctions, protect a client regime, secure a contract, normalize a technology vendor, or make democratic resistance look futile.

Natural-language indicators analysts should watch

Natural-language processing can help identify the fingerprint without judging political viewpoint. Analysts should look for unusual phrase convergence across supposedly independent outlets; high semantic similarity after translation or localization; synchronized publication bursts; identical named-entity pairings; repeated emotional triggers; and a diffusion pattern that moves from state media or obscure portals into local commentary and then back into mainstream coverage. These indicators do not prove control. They identify where provenance, funding, and coordination require human investigation. The objective is attribution, not automated censorship.

Russia: Outsource the message, localize the grievance

Moscow's comparative advantage is not making Russia attractive. It is making democratic confidence expensive. The Internet Research Agency case showed the template. Beginning in 2014, Russian operators allegedly used false American identities, social media pages, paid advertisements, and even locally organized events to wage what their own documents called information warfare against the United States. The 2018 indictment described an effort to spread distrust of candidates and the political system itself (U.S. Department of Justice, 2018).

The method did not disappear. It professionalized. In 2023, the U.S. Department of State exposed a Kremlin-funded plan to use media contacts across at least thirteen Latin American countries. Russian

teams would create content, Spanish- and Portuguese-speaking intermediaries would localize it, and regional editorial contacts would publish it so the material appeared organic. The named Russian firms included the Social Design Agency and Structura. In 2024, the U.S. Treasury sanctioned those firms and their leaders for Kremlin-directed malign influence, and the Justice Department seized thirty-two internet domains associated with the related Doppelganger operation. The court filings described cybersquatted news sites, fabricated personas, paid advertising, influencers, and synthetic content targeting the United States, Mexico, and other audiences (U.S. Department of Justice, 2024a; U.S. Department of State, 2023; U.S. Department of the Treasury, 2024).

A second 2024 case alleged that employees of the Russian state-controlled outlet RT routed nearly \$10 million through a Tennessee-based content company that published thousands of videos and gained millions of views. The allegations are charges, not convictions, and they do not establish that every commentator knew the money's origin. That is precisely the point. A covert sponsor gains more legitimacy when the public face believes the content is his own (U.S. Department of Justice, 2024b).

Russia's Latin American strategy adapts familiar themes to local memory: U.S. imperialism, NATO aggression, sanctions as collective punishment, and Moscow as a champion of a multipolar Global South. The content works best when it does not sound Russian. It sounds Chilean, Mexican, Brazilian, Colombian, or Venezuelan. The local voice is not decoration. It is the delivery system.

China: Borrow the boat, own the current

Beijing generally plays a longer game. Russian operations often seek collision. Chinese Communist Party influence more often seeks accommodation, control of the agenda, self-censorship, and the normalization of dependency. The Party's own logic is captured in the phrase "borrow a boat to go out to sea": use an established local platform to carry a state narrative farther and with greater credibility than overt propaganda could travel on its own (National Endowment for Democracy, 2024; Reporters Without Borders, 2026).

Across Latin America, that boat can be a content-sharing agreement, a paid supplement, a sponsored press tour, a university partnership, a business association, a diaspora outlet, or a public broadcaster. Reporters Without Borders found that Beijing is increasingly using established regional media as channels rather than competing solely through Chinese outlets. Separate studies document the same toolkit: journalism exchanges, coproductions, paid placements, diplomatic social-media accounts, and relationships with governors, mayors, universities, and commercial media (Freedom House, 2022; National Endowment for Democracy, 2024; Shullman, 2024).

The geoeconomic layer is central. Chinese policy banks supplied more than \$138 billion in loans to Latin America between 2005 and 2020, while regional trade with China reached \$445 billion in 2021. Those numbers do not make each loan or trade relationship malign. They explain why narrative access matters. A government that depends on a commodity buyer, a telecom vendor, a port operator, an electricity supplier, or a financing channel develops constituencies that will defend the relationship, sometimes before the public can examine its strategic terms (Shullman, 2024).

Panama illustrates the integration of money and messaging. Following diplomatic recognition of Beijing, Chinese state-linked entities developed content-sharing or paid-placement arrangements with mainstream Spanish-language media, while journalists participated in China-funded training trips. The promise of investment and access reinforced the preferred story: partnership with Beijing was modern, pragmatic, and inevitable (Freedom House, 2022; Shullman, 2024).

Canada demonstrates the sharper edge. The 2025 public inquiry concluded that foreign interference affected the broader electoral ecosystem and public confidence, even though it did not determine which party formed government in 2019 or 2021. In 2026, Canada's Rapid Response Mechanism reported a PRC-linked Spamouflage campaign targeting ten Mandarin-speaking individuals with doctored videos, doxing, and roughly 100 to 200 new posts per day. More than 5,000 posts produced little public engagement, a crucial analytic caveat: volume is capability, not proof of impact. Meta had previously dismantled a far larger Spamouflage network involving 7,704 Facebook accounts, 954 pages, 15 groups, and activity across more than fifty platforms (Global Affairs Canada, 2026; Meta, 2023; Public Inquiry into Foreign Interference, 2025).

China's method is therefore quieter, but not benign. It seeks to shape the boundaries of acceptable discussion, especially on Taiwan, Hong Kong, Xinjiang, Tibet, technology, and the legitimacy of authoritarian development. The strategic achievement is not always applauded. Sometimes it is silence.

Iran: Turn grievance into an echo chamber

Tehran operates with fewer resources than Moscow or Beijing, but its influence architecture is ideologically focused and increasingly fused with cyber operations. In July 2024, the U.S. Director of National Intelligence warned that actors tied to Iran were posing as activists online, encouraging Gaza-related protests, and in some instances providing financial support. The statement carefully emphasized that Americans expressing sincere views were not, by virtue of that, Iranian agents and might not know whom they were dealing with. That warning should be the democratic standard: expose the foreign manipulation without smearing legitimate protest (Office of the Director of National Intelligence, 2024; Reuters, 2024).

Two months later, the Justice Department charged three Islamic Revolutionary Guard Corps cyber actors in an alleged hack-and-leak operation designed to influence the 2024 U.S. presidential election. Microsoft independently documented Iranian operations that combined compromised accounts, covert social-media personas, and imposter news sites. The pattern is hybrid: steal information, selectively release it, wrap it in a moral story, and let domestic actors distribute the payload (Microsoft Threat Analysis Center, 2024; U.S. Department of Justice, 2024c).

In Latin America, Tehran's bridge is Spanish-language media and the Bolivarian information ecosystem. HispanTV, owned by the Islamic Republic of Iran Broadcasting, supplies an anti-U.S. and anti-Israel narrative calibrated to parts of the Latin American left. Research by the National Defense University and Dialogo Politico describes an echo chamber in which HispanTV, the Venezuela-based TeleSUR, RT en Español, allied websites, and social media accounts reinforce one another until a state narrative acquires the appearance of regional consensus (Castaño Riaño, 2024; Farah & Tavarez, 2021).

Venezuela, Cuba, and Nicaragua are more than passive relays. Their state-backed media and political networks localize extra-hemispheric narratives, use them to discredit the democratic opposition, and receive in return reciprocal legitimacy. A 2025 German Marshall Fund study of nearly 15,000 TeleSUR articles found a heavily asymmetric pattern: Western actors dominated negative coverage, while Russia and China received far less critical scrutiny. The study also noted that TeleSUR's publicly documented partnerships with Russian and Chinese outlets center on content sharing and co-production, not on direct financing. That distinction matters, but the amplification effect remains strategically useful (Sebares Jimenez-Blanco, 2025).

Same terrain, different destination

It is tempting to describe Russia, China, and Iran as one synchronized bloc. The evidence supports convergence, not uniformity. Moscow gains from disorder, alliance fatigue, and disbelief. Beijing gains from access, elite accommodation, technological position, and a world in which criticism of the Party carries economic cost. Tehran gains from ideological mobilization, pressure on U.S. support for Israel, sanctions resistance, and legitimacy for its revolutionary model and proxies. Their regional partners gain regime protection and an external explanation for domestic failure (Farah, 2025; Puyosa & Marin Vazquez, 2023).

Their messages often meet at the same junction: anti-colonial language, resentment of U.S. power, celebration of multipolarity, suspicion of liberal institutions, and the claim that sovereignty means freedom from scrutiny. None of those ideas is inherently foreign or illegitimate. Their operational value lies in selective application. U.S. failures are treated as proof that democracy is fraudulent. Russian aggression becomes resistance. Chinese state capitalism becomes neutral development. Iranian repression disappears behind the language of anti-imperialism.

This is where geopolitics meets geoeconomics. An information campaign can make a sanctions-evasion partner look principled, a surveillance platform look merely efficient, an opaque loan look generous, or a strategic port look like a purely commercial asset. Narrative capture lowers the political cost of market capture. It also raises the cost of reversal because local jobs, contracts, campaign relationships, and institutional reputations become tied to the foreign presence.

Strategic communication without economic delivery is theater. Economic statecraft without strategic communication is an invisible victory.

The United States, therefore, cannot fact-check its way out of a vacuum created by neglect. If Washington arrives only to warn, while Beijing arrives with financing, Moscow with a ready-made explanation, and Tehran with a moral cause, the adversaries control both the material and emotional tempo. An America First approach should begin with hemispheric presence: faster transparent financing, secure digital infrastructure, reliable energy and mineral partnerships, nearshoring, market access, and sustained Spanish- and Portuguese-language engagement. The best counternarrative is often a promise kept.

Key judgments

- **MSI² assesses (High Confidence):** The most effective foreign influence operations do not manufacture audiences from nothing. They attach themselves to authentic grievances and pass through trusted local intermediaries, making provenance more decisive than ideology.
- **MSI² assesses (High Confidence):** Russia, China, and Iran pursue different strategic outcomes, but they benefit from the same vulnerabilities: opaque funding, weakened local journalism, fragmented platforms, low institutional trust, and economic relationships that discourage scrutiny.
- **MSI² assesses (Moderate Confidence):** Foreign services can move a person along a continuum from unwitting amplification to privileged access, cultivation, and witting tasking by combining financial opportunity, ideological affinity, compromise, and ego. The transition is usually incremental and is best detected through patterns of concealment, dependency, unusual requests, and repeated boundary crossings rather than personal association alone.

- **MSI² assesses (Moderate Confidence):** As competition over ports, telecommunications, energy, critical minerals, data, and logistics intensifies, geoeconomic dependency will increasingly shape which foreign narratives local elites and institutions are willing to challenge.
- **MSI² assesses (High Confidence):** Broad censorship or viewpoint policing would undermine democratic legitimacy and provide adversaries with fresh propaganda. Transparency, attribution, narrow enforcement against deceptive conduct, independent media, and preemptive public education are more durable defenses.

Policy recommendations

1. **Defend the line between dissent and interference.** Base government action on conduct, provenance, coercion, deception, and unlawful foreign direction, not on ideology or policy position. Publish evidentiary standards and provide due-process protections.
2. **Make provenance visible at the speed of the feed.** Require durable disclosure for foreign state-funded media, paid political content, sponsored research, content-sharing arrangements, and synthetic personas. Platforms should preserve public archives of coordinated inauthentic networks and share indicators with qualified researchers.
3. **Create a Shield of the Americas Information Integrity Compact.** Link U.S., Canadian, Latin American, and Caribbean partners in a standing fusion mechanism for technical attribution, campaign finance intelligence, foreign-agent transparency, sanctions enforcement, diaspora protection, and rapid multilingual public exposure.
4. **Follow the money into the narrative.** Integrate beneficial ownership, foreign-agent registration, procurement integrity, academic funding disclosure, and strategic-investment review. Ports, telecom networks, electricity grids, data centers, media ownership, and critical-mineral projects require security review before dependency hardens into political leverage.
5. **Compete with delivery, not lectures.** Pair warnings about authoritarian leverage with credible alternatives: faster development finance, risk insurance, secure digital infrastructure, nearshoring incentives, transparent public-private partnerships, and market access. A partner who is offered no alternative has not been given a strategy.
6. **Rebuild independent hemispheric journalism.** Fund a firewalled, nonpartisan investigative capacity in Spanish and Portuguese, including regional correspondents who can report directly on China, Russia, and Iran. Support should protect editorial independence and favor local ownership over Washington-produced messaging.
7. **Prebunk the playbook.** Teach citizens how impersonation, source laundering, emotional loading, hack-and-leak operations, doxing, and coordinated amplification work before a crisis. Research shows that psychological inoculation can improve resistance to manipulation without telling people what political conclusions to reach (Roozenbeek et al., 2022).
8. **Train the people most likely to be cultivated.** Provide role-specific counterintelligence awareness and confidential reporting channels for elected officials and staff, journalists, academics, researchers, technology executives, defense contractors, diaspora leaders, and personnel with access to strategic infrastructure. Training should explain elicitation, gifts, paid travel, private introductions, romantic cultivation, escalating favors, and coercion without treating normal foreign contact as suspicious.
9. **Impose costs on the hidden hand.** Use targeted sanctions, domain seizures, criminal prosecution, visa restrictions, and asset tracing against foreign operatives, front companies, and knowing intermediaries. Protect unwitting participants and reserve punishment for evidence-backed misconduct.

Key takeaways

- The phrase may be misattributed to Lenin, but the operational concept is real: a foreign power can gain strategic utility from people who do not understand the sponsor or end state.
- The test is not whether speech is offensive, radical, progressive, conservative, isolationist, or anti-establishment. The test is whether a foreign hand is covert, deceptive, coercive, criminal, or deliberately concealed.
- Russia seeks paralysis, China seeks normalization and leverage, Iran seeks mobilization, and aligned regional regimes help all three localize their messages.
- Economic dependency and information dependency reinforce one another. Contracts create advocates; narratives protect contracts.
- MICE explains the recruitment threshold: money, ideology, compromise, and ego can turn access into dependence and dependence into tasking, but association alone is not evidence of control.
- Open societies should not become less open. They should become harder to deceive and more capable of delivering visible results to their own citizens and partners.

The lights must stay on

Lioness works because it turns an invisible system into a human story. Real life is harder. There is rarely one professor, one payment, one handler, or one clean chain of command. There may be a paid trip, a person who listens at precisely the right moment, a favor that seems too small to matter, or a relationship that changes one boundary at a time. Influence moves through partial knowledge, mixed motives, social prestige, commercial incentives, and genuine conviction. That ambiguity is not a reason to ignore the threat. It is a reason to investigate it with discipline.

The enemy does not need to break down the gate if citizens, institutions, and markets can be persuaded to hold it open. However, the democratic answer cannot be to seal the gate and extinguish debate. That would convert defense into self-defeat.

The answer to the army without uniforms is not an army of censors. It is a republic of citizens who know who is speaking, who is paying, how a story traveled, and what strategic outcome their outrage may be serving. Keep the society open. Turn on the lights. Expose the hand on the scale.

Analytic note

Analytic cutoff: September 2, 2026. This essay uses public-source reporting and does not infer individual culpability from viewpoint alignment. Each operational case is supported by at least two evidence streams, including public court records or official findings and separate technical, academic, or investigative analysis. Allegations drawn from indictments are identified as allegations. Campaign scale or activity volume is not treated as proof of audience impact.

References

- Boller, P. F., Jr., & George, J. (1989). They never said it: A book of fake quotes, misquotes, and misleading attributions. Oxford University Press.
- Brady, W. J., Wills, J. A., Jost, J. T., Tucker, J. A., & Van Bavel, J. J. (2017). Emotion shapes the diffusion of moralized content in social networks. *Proceedings of the National Academy of Sciences*, 114(28), 7313-7318. <https://doi.org/10.1073/pnas.1618923114>
- Burkett, R. P. (2013). An alternative framework for agent recruitment: From MICE to RASCLS. *Studies in Intelligence*, 57(1), 7-17. Central Intelligence Agency. <https://www.cia.gov/resources/csi/studies-in-intelligence/volume-57-no-1/an-alternative-framework-for-agent-recruitment-from-mice-to-rascls/>
- Canadian Security Intelligence Service. (2021, July). Foreign interference threats to Canada's democratic process. Government of Canada. <https://www.canada.ca/en/security-intelligence-service/corporate/publications/foreign-interference-threat-to-canadas-democratic-process.html>
- Castaño Riaño, S. (2024). Iran's soft power in Latin America: HispanTV. *Dialogo Politico*. <https://redaccion.dialogopolitico.org/wp-content/uploads/2024/05/DP-Enfoque-15.-Irans-soft-power-in-Latin-America.pdf>
- Farah, D. (2025). Trilateral authoritarian alliance and the People's Republic of China. Florida International University, Jack D. Gordon Institute for Public Policy. <https://digitalscholarship.fiu.edu/record/19467>
- Farah, D., & Tavaréz, A. (2021). Iran in Latin America: Malign alliances, 'super spreaders,' and alternative narratives (Strategic Perspectives 34). National Defense University Press. <https://www.ndu.edu/News/Article-View/Article/2643486/>
- Foreign Malign Influence Center. (2024). FMI primer: An introduction to foreign malign influence. Office of the Director of National Intelligence. https://archive.dni.gov/files/FMIC/documents/products/04-25-24_Report_FMI-Primer-Public-Release.pdf
- Freedom House. (2022). Beijing's global media influence 2022: Authoritarian expansion and the power of democratic resilience. <https://freedomhouse.org/report/beijing-global-media-influence/2022/authoritarian-expansion-power-democratic-resilience>
- Global Affairs Canada. (2026, May 11). Canada targeted in a new Chinese transnational repression campaign linked to 'Spamouflage.' <https://international.canada.ca/en/global-affairs/corporate/reports/rapid-response-mechanism/news/2025-china-spamouflage>
- Green, M. C., & Brock, T. C. (2000). The role of transportation in the persuasiveness of public narratives. *Journal of Personality and Social Psychology*, 79(5), 701-721. <https://doi.org/10.1037/0022-3514.79.5.701>
- Meta. (2023). Meta's adversarial threat report, second quarter 2023. <https://transparency.meta.com/sr/Q2-2023-Adversarial-threat-report/>
- Microsoft Threat Analysis Center. (2024, August 9). Iran steps into U.S. election 2024 with cyber-enabled influence operations. <https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf>
- National Protective Security Authority. (2025, April 1). Think before you link. <https://www.npsa.gov.uk/resources/protective-security-guidance-think-you-link>
- National Endowment for Democracy. (2024, May 2). Borrowing boats: How are key influencers in Latin America amplifying CCP narratives about authoritarian models? <https://www.ned.org/borrowing-boats-how-are-key-influencers-in-latin-america-amplifying-ccp-narratives-about-authoritarian-models/>
- Office of the Director of National Intelligence. (2024, July 9). Statement from Director of National Intelligence Avril Haines on recent Iranian influence efforts. <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2024/3784-statement-from-director-of-national-intelligence-avril-haines-on-recent-iranian-influence-efforts>
- Paramount+. (2026, August 30). The Idiot Army (Season 3, Episode 5) [TV series episode]. In *Lioness*. <https://www.paramountplus.com/shows/lioness/episodes/>
- Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions. (2025). Final report, volume 1. Privy Council Office. https://publications.gc.ca/collections/collection_2025/bcp-pco/CP32-169-2-2025-eng-1.pdf
- Puyosa, I., & Marin Vazquez, M. (2023). Deepening the response to authoritarian information operations in Latin America. National Endowment for Democracy. <https://www.ned.org/deepening-the-response-to-authoritarian-information-operations-in-latin-america/>
- Reporters Without Borders. (2026, March 16). 'Instead of competing with local media, China uses them as channels': Beijing's media strategy in Latin America. <https://rsf.org/en/instead-competing-local-media-china-uses-them-channels-beijing-s-media-strategy-latin-america>

- Reuters. (2024, July 9). White House warns Iran against meddling in Gaza protests in U.S. <https://www.reuters.com/world/us/white-house-warns-iran-meddling-gaza-protests-us-2024-07-09/>
- Roozenbeek, J., van der Linden, S., Goldberg, B., Rathje, S., & Lewandowsky, S. (2022). Psychological inoculation improves resilience against misinformation on social media. *Science Advances*, 8(34), eabo6254. <https://doi.org/10.1126/sciadv.abo6254>
- Safire, W. (1987, April 12). On language: Useful idiots of the West. *The New York Times*.
- Sebares Jimenez-Blanco, M. (2025, April 9). Venezuela through the Sino-Russian media playbook. German Marshall Fund of the United States. <https://www.gmfus.org/news/venezuela-through-sino-russian-media-playbook>
- Shapiro, F. R. (2019, August 22). Phrase origin: Useful idiot. *Quote Investigator*. <https://quoteinvestigator.com/2019/08/22/useful-idiot/>
- Shullman, D. O. (2024, February 12). China pairs actions with messaging in Latin America. The United States should do the same. Atlantic Council. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/china-pairs-actions-with-messaging-in-latin-america-the-united-states-should-do-the-same/>
- U.S. Department of Justice. (2018, February 16). Grand jury indicts thirteen Russian individuals and three Russian companies for scheme to interfere in the United States political system. <https://www.justice.gov/archives/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere>
- U.S. Department of Justice. (2024a, September 4). Justice Department disrupts covert Russian government-sponsored foreign malign influence operation targeting audiences in the United States and elsewhere. <https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence>
- U.S. Department of Justice. (2024b, September 4). Two RT employees indicted for covertly funding and directing U.S. company that published thousands of videos in furtherance of Russian interests. <https://www.justice.gov/archives/opa/pr/two-rt-employees-indicted-covertly-funding-and-directing-us-company-published-thousands>
- U.S. Department of Justice. (2024c, September 27). Three IRGC cyber actors indicted for 'hack-and-leak' operation designed to influence the 2024 U.S. presidential election. <https://www.justice.gov/usao-dc/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us>
- U.S. Department of State. (2023, November 7). The Kremlin's efforts to covertly spread disinformation in Latin America. <https://2021-2025.state.gov/the-kremlins-efforts-to-covertly-spread-disinformation-in-latin-america/>
- U.S. Department of the Treasury. (2024, March 20). Treasury sanctions actors supporting Kremlin-directed malign influence efforts. <https://home.treasury.gov/news/press-releases/jy2195>
- Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146-1151. <https://doi.org/10.1126/science.aap9559>