MITRE | Intelligence After Next

2025 PRESIDENTIAL TRANSITION SPECIAL EDITION

COUNTERING MALIGN MESSAGING AND INFLUENCE CAMPAIGNS: WE NEED A HOLISTIC RESPONSE

by John Rodman

As part of MITRE's support to the 2025 Presidential transition, we are highlighting key Intelligence After Next (IAN) papers published recently to stimulate thought, dialogue and action for intelligence and national security leaders. Key topic areas include surveillance, privacy, transparency, and accountability; foreign policy; counterterrorism and cybersecurity strategies; combatant command support; and the future of the IC workforce. IAN papers aligned to these topic areas address key policy, acquisition and warfighting concerns and are as relevant in 2025 as when first published.

A Holistic Approach to Counter Messaging and Influence

The Government Accountability Office (GAO) reported in its 2021 testimony to Congress that "neither the U.S. government (as a whole) nor DoD (as a department) have a definition for "information warfare." Efforts to counter the effects of information operations (IO)—which include messaging to influence—are increasing in many agencies, with competing authorities and missions. Yet, capable adversaries with quite different operating rules run highly adaptive IO programs that take advantage of the propagation and interaction of information (interactivity, sharing, and reposting) and the potential for scaling from seedling operations to national-level campaigns.[1] U.S. efforts to counter these campaigns will have marginal success without a coordinated, national IO campaign that assesses the threat, develops effective responses, and implements aligned solutions. A national program must deter an adversary's influence, counter the effectiveness of their IO efforts, and create a counter narrative. Integrating these aspects nationally requires being:

- Holistic when looking at the intent, capabilities, and messaging connectedness of actors and actions to understand the attack vectors and likelihood of success
- Strategic in shaping our adversaries' actions, open enough to engender public trust, true to our values, and legally compliant
- Predictive so the United States can create an information environment where our adversaries' messaging finds a less receptive audience

The necessity to counter IO will continue as other nations try to gain advantage in their decision space or disadvantage the U.S. by creating chaos, delaying U.S. actions, or increasing ambiguity. Technology and ubiquitous information access increase the speed, spread, and tenacity of messaging used to influence. Our adversaries' information operations depend on how cheaply, quickly, and widely they can confuse or clutter the information space; exploit big data and technology to focus messaging; and marshal national resources for a sustained, multi-dimension influence campaign. Countering these trends is a multi-pronged problem of:

- Managing counter IO processes by reconciling authorities, resources, and roles
- Gaining control of the narrative space by deconflicting U.S. messaging efforts
- Dominating the data management in this seemingly spontaneous environment by building an IO knowledge base, critical technology, and the requisite workforce

Three challenges shape the U.S. counter messaging and influence campaigns: the ability to deter, counter, and create influence.

- **Deterring Influence:** Creating an influence-savvy population is a comprehensive and resourceintensive effort that cannot be heavy-handed or uninformed. Success is hard to measure, but research on assessing resilience is increasing and improving with data.
- **Countering Influence:** While essential, there is a "stickiness" to messaging that is designed to resonate with target audiences' biases. It is also hard to get a counter message out with sufficient scale, scope, and speed unless the government controls the media. Although success rates can be low, U.S. government saw some success with the release of classified intelligence to debunk or expose Russia's IO.

- Creating Influence: Campaigns may focus on government (including military) influence or more comprehensive political-social-technical influence operations (i.e., China or Russia). U.S. counter IO must align with public education and defensive mechanisms, and have operational speed, sufficient authorities, an agile structure, and sustainable resourcing.

Defining Messaging and Influence Operations

Shaping an adversarie's decision environment through open and hidden means is as old as human conflict, but the scale, scope, and speed of influence operations have changed drastically in the past decade. We now must confront more automated and autonomous digital methods, expanded use of online and real proxies, and highly convincing conspiracy-based information warfare that can include deep fakes and artificial intelligence-generated content. IO recently conducted against the U.S. and shared with the public include targeting government officials and citizens through traditional intelligence tradecraft; criminal efforts to suppress voting and supply illegal campaign financing; and cyber attacks against voting infrastructure and computer intrusions targeting elected officials and others.[2] The Department of Defense created in 2022 a center for developing understanding and possible responses to irregular warfare, of which IO is a part, but it is initially focused on allied security cooperation and education rather than managing the DoD response. This effort will help define the issue and mission space for DoD, but not civilian agencies and departments involved in countering IO.[3]

Objectives of Messaging and Influence Campaigns

An actor, state or nonstate, strives to create conditions favorable to their strategic goals by manipulating intelligence, diplomatic, economic, military, political, cultural, and social information. Often technology enabled, the adversary systematically creates ambiguity, manages information and its flow, or falsifies data to delay or misdirect actions.

FOREIGN MALIGN INFLUENCE (50 U.S. CODE § 3059):

"The term 'foreign malign influence' means any hostile effort undertaken by, at the direction of, or on behalf of or with the substantial support of, the government of a covered foreign country with the goal of influencing, through overt or covert means—

(A) the political, military, economic, or other policies or activities of the United States Government or State or local governments, including any election within the United States; or

(B) the public opinion within the United States."

Influence campaigns may include propaganda and disinformation, involve multiple official and nonofficial actors, and have complementary and contradictory messages interwoven as needed. Messaging campaigns to influence another nation are a balancing act between focused, directed, and surgical messaging toward key decision makers or influential sectors of a nation and creating societal discord or shaping through less controllable messaging. Broadly, an adversary's messaging efforts have the following components:

- **Support Strategic Goals:** An adversary uses their knowledge to shape an opponent's foreign policy to help their interests by manipulating perceptions and biases in that country or internationally.
- **Strategic Deterrence and Threat:** An adversary hides or misrepresents the status of nuclear programs, weapons of mass destruction, advanced weapons, or strategic relationships to gain.
- **Information Campaigns:** An adversary creates complex, sequenced injections to shape behavior, sow misinformation to confuse and misdirect, and build national influence campaigns.

- **Information Channels/Feedback Loops:** An adversary manipulates an opponent to see how they react, construct better feedback loops, or find better influence channels.

The Drivers and Enablers of Messaging and Influence

The components of an influence campaign are mixed, played, and removed based on the strategic goals, short-term adjustments, and ever-changing knowledge our adversaries have of the United States. Other considerations are the best method of conveying the message to a single or multiple targets, and how feedback is gathered.

With an influence campaign, an adversary can create chaos; delay an opponent taking timely action; and even cause a misstep in political, economic, or military decisions by increasing ambiguity or selectively decreasing it. While manipulating perceptions is not always dependent on advanced technology, technology is an important enabler because digital formats, tools, and access can shape behavior with less cost and risk, while also potentially offering information about the targets via monitored information feeds.

Some messaging actions are controlled, but many are sent into the "information wilds" to develop a life of their own. If the knowledge of the adversary is good, shaping outcomes may be accomplished. If the scale, scope, and resonance of misinformation and disinformation are overwhelming, then delay and confusion may be a force multiplier. Messages can start or end at any time or with any audience and can morph from highly focused to broad societal targeting and back to target newly formed influence groups depending on feedback. This requires our adversaries to constantly react to current events in the U.S. and its partners. The more specific the target and message, the more preparation and knowledge are required. For our adversaries to succeed in shaping outcomes, not just sowing chaos, it is essential that their messaging is sufficiently believable, verifiable, or consistent to the target audience.

The Need for a Coordinated Counter Messaging Campaign

Messaging and influence are part of the policy, institutions, and modus operandi for Russia and China. They are identified throughout our national strategies as the primary security challenges for our nation. Russia has conducted propaganda, information campaigns, and active measures since the 1920s to undermine internal institutions to support the communist takeover[4] and to villainize the West when advantageous. China sees the "divine manipulation of the threads," which includes the spreading of disinformation,[5] as a primary tool of government against its enemies since Sun Tzu. A Harvard review of 223 IO countermeasures studies since 1972 identified four essential factors that contribute to successfully countering influence operations: Assessing the impact on real-world behaviors (online and offline) to improve IO Improving the efficacy of countermeasures in non-Western contexts Finding and targeting creators of disinformation Improving a nation's information consumers.[6]

The key components identified in this paper—deterring, countering, and creating influence—encapsulate and expand on these essential factors of the last 50 years.

The government is tackling how to assess impact, but there are privacy, ability, industry, and response barriers to overcome. We may improve our countermeasures through diverse academic and analytic inspection, combined with the government's authorities and operational lessons learned.

Finding and targeting the creators of mis/disinformation are difficult because of the current fractured nature of federal efforts that inhibit our ability to create counter messaging plans. The government and private industry are improving public awareness with varying levels of informal and formal coordination, but challenges remain.

- U.S. Cyber Command, Department of Homeland Security (DHS), Department of State, and Federal Bureau of Investigation all claim a measure of primacy in countering influence.[7] Among the

many players, a more strategic, holistic approach is needed. In 2022, the DHS Office of Inspector General determined that the rapid and disjointed creation of entities to counter influence requires a unified strategy to counter social media disinformation campaigns.[8]

- The 2020 Intelligence Authorization Act required the Office of the Director of National Intelligence (ODNI) to establish a body for coordinating intelligence from across the 18 Intelligence Community members on hostile foreign influence campaigns. However, this small, nascent group—the Foreign Malign Influence Center (FMIC)—from its inception has been questioned for its potential duplication of existing efforts, particularly those of the Global Engagement Center (GEC) at the Department of State and multiple DHS efforts.[9]

For two decades, reviews of our national security process have called for increased understanding of the influence of social networks (2008),[10] creating a centralized counter messaging capability (2019),[11] and sorting out the "real" from "not real" in influence operations (2021).[12] The U.S. government response was providing funding to individual organizations, which did not produce a centralized counter messaging capability and may have created multiple interpretations of social networks and influence operations.

Values, Efficacy, and Necessity

The ethics of countering foreign influence (i.e., our values) shape how a nation determines the efficacy (i.e., likelihood of success) and lead to the question of how the U.S. government should measure the effectiveness of countering influence. Some barriers to measuring counter influence operations' efficacy may complicate the investment in national countermeasures.

- Measuring the effectiveness of countermeasures may be difficult to quantify due to the time lags associated with an influence operation's impact, attribution of originator or source, and a lack of standards for determining influence.
- Reducing the effectiveness of an influence operation through fact-checking, "prebunking" (preemptively refuting misinformation narratives), increasing literacy on accuracy in the media, and crowdsourcing the identification of misinformation have proved to be insufficient alone or in tandem.[13]
- Understanding the impact of influence through social media requires a high level of audience response because overstating the threat can reduce trust and result in rejection of future warnings. Public and private fact-checking needs to be accurate, accessible, and visually appealing.[14]

Building Sustainable Counter IO

To counter adversary IO, the U.S. needs to bolster resistance to nefarious messaging, employ a methodical and anticipatory national response mechanism, and generate influence that puts our adversaries on the defensive. Our ability to impose disincentives, or cost-imposing counter messaging strategies against adversaries, requires understanding how they perceive and calculate risks.[15] We must be able to detect foreign influence operations, distinguish between benign and malign activity,[16] and understand the danger imposed to the U.S. while also determining the most effective counters. This may require an independent review effort charged with developing actionable recommendations for leveraging current capacity, reimagining our processes, and identifying innovative ways to counter and create influence.

Manage Processes: Reconcile authorities, resources, and roles to create an integrated, resilient, and trusted counter messaging process.

Recommendations:

- Evaluate our current structure as a precursor to a comprehensive national counter messaging and influence capability.
- Create a dedicated budget for a nationally coordinated counter IO campaign[17] to fund critical needs like educating the public and common counter influence capabilities.[18]
- Reimagine the capacity, functions, and roles of assets like the FMIC, the National Counterintelligence and Security Center, the National Media Exploitation Center, and current Department of Defense and Intelligence Community capabilities.

Control Narratives: Create a U.S. narrative with deconflicted messaging through coordinated dispersal with rapid feedback, analysis, and response.

Recommendations:

- Leverage mass media, social media, and international bodies as effectively as our adversaries through an integrated program to counter manipulation of our national interests.
- During the Cold War, the U.S. countered IO with coordinated efforts like the Active Measures Working Group,19 and we must create a 21st century counterpart.[20]
- Coordinate engagement processes to build coalitions in the government and throughout private industry. Unlike authoritarian regimes, the United States cannot control the information landscape, nor directly or indirectly finance proxies to manipulate media.
- Minimize inconsistent or poorly constructed messaging to reduce insights into U.S. capabilities and intentions that adversaries may use against us. We should use inconsistent messaging only to intentionally create ambiguity.[21]

Dominate Data: Curate and exploit the necessary data that can build an IO knowledge base, develop technical capabilities, and employ a specialized workforce to anticipate and counter narratives.

Recommendations:

- Find and use pertinent data to understand our adversaries' influence campaign attributes; strategic intent; and tactics, techniques, and procedures (TTPs). Using this data and information requires faster sharing and collaboration with tools designed to detect changes in messaging and leverage social media.[22]
- Rethink how to integrate and orient education, resilience, and operational components around data veracity of restricted and public information that may be concurrently used in IO. The counter IO workforce will need more agility, access, and outside engagement that is accountable, yet flexible.
- Give our future IO professionals the latitude to seriously "game" the opposition and introduce likelihoods of their next steps and ours into a counter IO program. Anticipating foreign malign messaging and influence requires an understanding of U.S. actions and the adversary's perceptions and reactions.

The U.S. has conducted counter IO programs during war and perceived existential crises, with both brilliant successes and marginal results. It is a reality of using influence as a national power that we must be willing to accept failures and missteps along with successes.

Acting on the challenges and needs identified in this paper is critical to countering unwanted and malign influence, a challenge occurring at an increasing pace and scale.

References

1. Mattheis, Garten-Ross, Koduvayur, Willson. February 2023. Blind Sided: A Reconceptualization of the Role of Emerging Technologies in Shaping Information Operations in the Gray Zone. Irregular Warfare Center.
2. FBI. FBI Director Christopher Wray's Statement at Press Briefing on Election Security. FBI News Online. August 2, 2018.
3. Cleveland, Egel, Howard, Maxwell, Rothstein. November 7, 2022. The Congressionally Authorized Irregular Warfare Center Is a Holistic Opportunity: Will the Department of Defense Capitalize on It? Rand Corporation.
4. Atran, Davis, Davuls. January 30, 2020. It Takes Social Science to Counter the Power of Russia's Malign Influence Campaign. Minerva Research Institute.
5. Sun Tzu. 500 BCE. The Art of War.
6. Harvard Kennedy School. September 13, 2021. Review of Social Science Research on the Impact of Countermeasures Against Influence Operations.
7. Department of State. May 17, 2022. Global Engagement Strategy Functional Bureau Strategy.
8. DHS Office of Inspector General. August 10, 2022. DHS Needs a Unified Strategy to Counter Disinformation Campaigns. OIG-22-58.
9. Klippenstein. May 5, 2023. The Government Created a New Disinformation Office to Oversee All the Other Ones. The Intercept (online).
10. Center for the Study of the Presidency. Forging a New Shield. Project National Security Reform. November 01, 2008.
11. Hatch. 2019. The Future of Strategic Information and Cyber-Enabled Information Operations. Journal of Strategic Security, Vol. 12 No. 4 Article 4.
12. Technology and Intelligence Task Force. January 2021. Maintaining the Intelligence Edge, Reimagining and Reinventing Intelligence through Innovation. Center for Strategic and International Studies.
13. Courchesne, IL Hardt, Shapiro. September 2021. Review of Social Science Research on the Impact of Countermeasures against Influence Operations. Misinformation Review, Princeton University, Empirical Studies of Conflict Project.
14. Mantzarlis, Alexios. The Secret to Live Fact-Checking? Be Very, Very Prepared. Poynter Institute for Media Studies. January 12, 2016.
15. Pillsbury. October-November 2012. The Sixteen Fears: China's Strategic Psychology. Survival: Global Politics and Strategy, Edition 54, No. 5,
16. Schoen, Lamb. 2012. Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference. National Defense University, Institute for National Strategic Studies, Strategic Perspectives 11. Washington D.C.
17. Hodges. February 10, 2021. Bureaucratizing to Fight Extremism in the Military. War on the Rocks.
18. Stockton. 2021. Defeating Coercive Information Operations in Future Crises. National Security Perspective, Johns Hopkins.
19. Schoen, Lamb. 2012. Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference. National Defense University, Institute for National Strategic Studies, Strategic Perspectives 11. Washington D.C.
20. Psychological Defense Agency. May 2023. Mission Statement. Sweden.
21. McCants, Wats. July 13, 2015. Can the United States Counter ISIS Propaganda? Brookings Institute.
22. Paul, Matthews. 2016. The Russian "Firehouse of Falsehood" Propaganda Model. RAND.

Author

John Rodman is a principal strategist in Enterprise Intelligence Solutions at MITRE. Previously a senior analyst at the CIA and U.S. Navy, he was also chairman of the Foreign Denial and Deception Committee on the National Intelligence Council.

Intelligence After Next

MITRE strives to stimulate thought, dialogue, and action for national security leaders developing the plans, policy, and programs to guide the nation. This series of original papers is focused on the issues, policies, capabilities, and concerns of the Intelligence Community as it prepares for the future. Our intent is to share our unique insights and perspectives surrounding a significant national security concern, a persistent or emerging threat, or to detail the integrated solutions and enabling technologies needed to ensure the success of the Intelligence Community. The views expressed in this publication are those of the author(s) and do not imply endorsement by the Office of the Director of National Intelligence or any other U.S. government department/agency.

You can receive all of MITRE's Intelligence After Next papers by subscribing to the series at mitre.org/IntelligenceAfterNext

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded research and development centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

JUNE 2023