Sarcouncil Journal of Arts Humanities and Social Sciences

ISSN(Online): 2945-3488

Volume- 04| Issue- 9| 2025

Review Article

Received: 30-07-2025 | Accepted: 20-08-2025| Published: 16-09-2025

Countering Foreign Influence: The Role of Strategic Communications in National Security Policy Making in the United States

Mohammed Hafiz Nabila[1], and Matilda Thompson[2]

[1]*East Tennessee State University, Johnson City, TN, USA*

[2]*Department of English, University of Ghana, Ghana*

Abstract:. Foreign influence operations executed as acts of disinformation pose critical national security challenges to the United States. Adversaries including China, Russia and Iran, have deployed disinformation to undermine democratic institutions and foment societal upheaval. These adversaries of the United States have weaponized Artificial Intelligence to execute sophisticated information warfare aimed at undermining the U.S., its allies, and interests. This analysis examines how strategic communications framework can build systems of resilience against foreign malign influence. The paper incorporates perspectives from European regulatory approaches to make recommendations that address America's situation. The analysis highlights a unified interagency approach, and public and private sector cooperation in countering disinformation threats. The paper identifies institutional capacity challenges, legal constraints from First Amendment safeguards, and the pace of technological advancements. The findings indicate that fragmented governmental responses contribute to persistent disinformation activities. A centralized strategy can enhance detection and attribution capabilities. The findings contribute to national security strategies in policymaking against evolving information warfare threats. The analysis offers insights for protecting U.S. national security, interests, and global positioning in the information environment.

Keywords: Disinformation, National security policymaking, Foreign Influence, Strategic communications, Information Warfare

INTRODUCTION

Defense strategic communication is a vital aspect of policy formulation for national security in the United States. Advancements in technology and competing political and economic interests have resulted in sophisticated foreign influence operations by enemies of the United States. Technological evolution has allowed foreign actors to carry out widespread attacks that are difficult to detect and trace.

The discovery of the Amarna letters provided insight into the early practice of international diplomacy. This document, which was found in Egypt, showed how the leaders of "Iraq, Syria, Egypt, Turkey, and the Levant" formed a union while administering affairs of their kingdoms (Bolt, 2019). King Ashurbanipal of Mesopotamia's palaces, with their ornamental representations on the walls, exhibit the king's strategic communications. Combat victories against Egypt and present-day southern Iran, wars against Babylonia, his kingdom's economic might and achievements, and the depth and breadth of the intellectual repository of his kingdom were showcased. These delineations, as depicted by the Kingdom of Mesopotamia, were influence activities combining "coercion and persuasion" aimed at intimidating rival kingdoms (Bolt, 2019).

Bolt (2019) observes that one key element that has always been overlooked is that the constant refinement and adjustment of "persuasion and coercion" for civilizations is at the center of all human activities in the administration of power.

In examining foreign influence, the concept of foreign interference becomes apparent. A close look at the forms that influence, and interference take shows that while some authorities concentrate on information related to issues like cyber threats, disinformation, misinformation, and such online-related dangers, other methodologies also explore information-centered operations along with acts that affect economic activity, "migration exploitation" and "manipulation of international organizations" (Fridman, 2024). The United States Department of Homeland Security incorporates both the information threat and political perspectives (including commerce) in its view of interference (Cybersecurity and Infrastructure Security Agency (CISA, 2019).

Misinformation and disinformation, according to the National Intelligence Council (NIC), are distinguished by the purpose behind the information. While an enemy of the United States can distribute wrong information to misinform, it becomes disinformation when it is done deliberately to achieve the enemy's ulterior objectives (United States Department of Justice, Office of the Inspector General, 2024, p.1).

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

*Corresponding Author: Matilda Thompson

DOI- DOI- https://doi.org/10.5281/zenodo.17135544

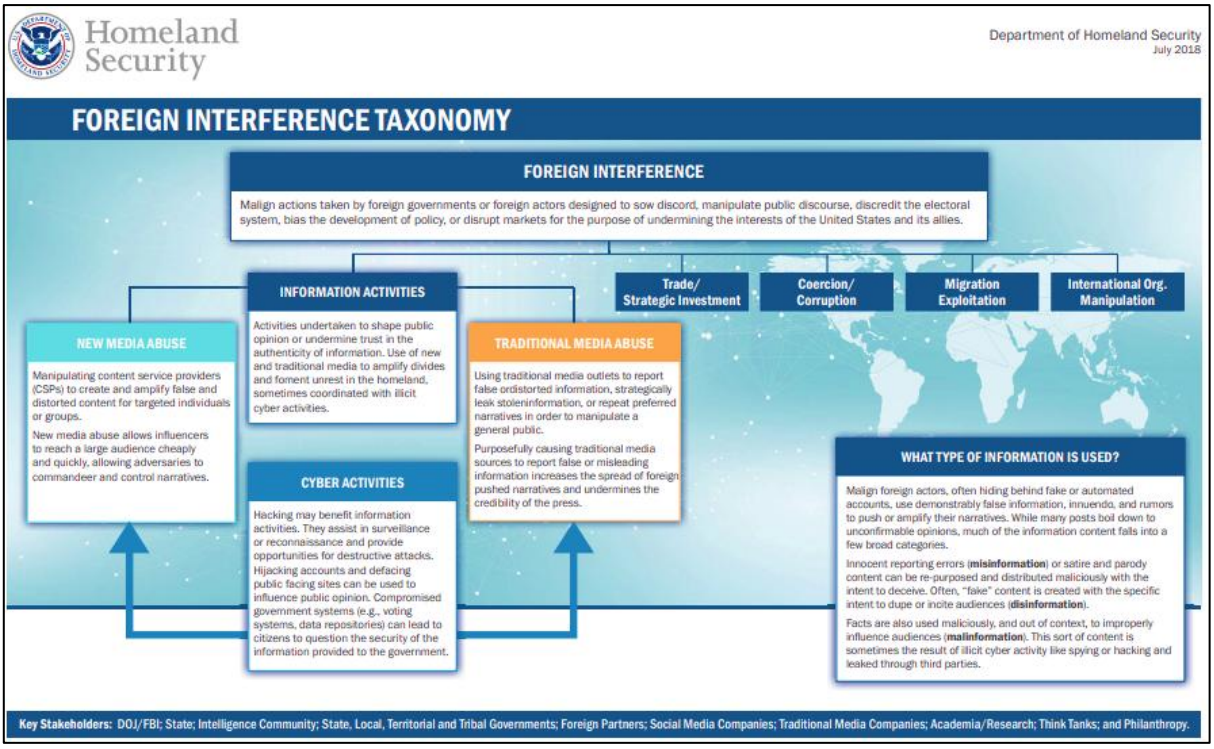


Figure 1: illustrates foreign interference as viewed by the U.S. Department of Homeland Security (CISA, 2019).

This paper focuses on the disinformation aspect of malign foreign influence, examines the actors and their strategies, and how strategic communication can be employed in national security policy to address information-related influence strategies that America's adversaries deploy.

KEY CONCEPTS

Strategic Communications

"Strategic communications entails the long-term shaping and shifting of significant discourses in societies. It adopts a holistic approach to communication based on values and interests that encompass everything an actor does to achieve objectives in a contested environment" (Bolt, 2019, p.4). The weaponization of disinformation in modern national security threats has changed how strategic communications must be understood and deployed, especially as adversaries take advantage of cognitive weaknesses and information ecosystems to undermine democratic institutions (Nabila & Thompson, 2025).

Althuis (2021, p.72) defines strategic communications as "the aligning of words, images, actions, and policy by a political actor with the intent of achieving changes in attitudes and/or behaviour of a target audience."

Foreign Malign Influence

Foreign malign influence (FMI) is the "subversive, undeclared, coercive, or criminal activities by foreign governments, non-state actors, or their proxies to affect another nation's popular or political attitudes, perceptions, or behaviors to advance their interests" (Office of the Director of National Intelligence, n.d.; Byman, 2025, p.2). The difference between foreign influence and FMI is that foreign influence includes diplomatic and foreign relations activities, deals with trade and economic-related issues, and recognized advocacy (Federal Bureau of Investigation (FBI, 2024). The foreign entity engaged in these activities is known (FBI, 2024), so actions are attributable.

According to the U.S. Department of Justice Office of the Inspector General (2024, p.1), the Federal Bureau of Investigation's "training materials" foreign malign influence is "subversive, covert (or undeclared), coercive, or criminal activities by foreign governments, nonstate actors, or their proxies to sow division, undermine democratic processes and institutions, or steer policy and regulatory decisions in favor of the foreign actor's strategic objectives and to the detriment of its adversary."

Kahler (2024, p. 4) defines malign foreign influence as "intended to affect domestic politics through coercive, corrupting, deceptive, or

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

clandestine means. In examining foreign influence, Kahler posits that the outlook is not to block all foreign influence activities in the United States' affairs. However, the discourse is directed at identifying influence actors and how they operate (Kahler, 2024). According to Fridman (2024), discussions centered on foreign influence over the last 10 years have been anchored by 3 main concepts: "hybrid warfare", "gray zone", and "Foreign Information Manipulation and Interference (FIMI)".

Gray Zone

According to Hicks, *et al.,* (2019, p. 2), the Center for Strategic and International Studies defines the Gray Zone confrontations as "an effort or series of efforts intended to advance one's security objectives at the expense of a rival using means beyond those associated with routine statecraft and below means associated with direct military conflict between rivals. In engaging in a gray zone approach, an actor seeks to avoid crossing a threshold that results in open war."

"The gray zone is an operational space between peace and war, involving coercive actions to change the status quo below a threshold that, in most cases, would prompt a conventional military response, often by blurring the line between military and nonmilitary actions and the attribution for events" (Morris, *et al.*, 2019, pp. 7–8).

This perspective of influence threat has acquired widespread acceptance in the United States (Fridman, 2024). Disinformation falls under the Gray Zone concept, and for this paper, which examines foreign influence primarily with the context of the United States, the focus will be on this Gray Zone operation.

Understanding the interconnected nature of these concepts exposes how adversaries of the U.S. weaponize information spheres to take advantage cognitive weaknesses. They do these to undermine democratic institutions and processes.

FOREIGN INFLUENCE THREATS AGAINST THE UNITED STATES

China, Russia, and Iran are the main foreign influence threats that persist in activities aimed at discrediting the United States' democratic institutions and engineering societal discord (U.S. Department of Homeland Security, 2024). These nations will leverage further developments in Artificial Intelligence (AI) to escalate their activities in the information sphere, making them more sophisticated and difficult to detect and attribute (U.S. Department of Homeland Security, 2024). Hicks, *et al.,* (2019) classified Gray Zone activities from these three countries under five classifications: information operations and disinformation, political coercion, economic coercion, cyber operations, and space operations (Hicks, *et al.,* 2019).

China

With the help of AI and advancements in technology, China is making it more difficult to detect fake accounts online as part of its disinformation strategy. This operation is targeted at denigrating the United States on the global stage while simultaneously improving theirs (U.S. Department of Homeland Security, 2024). China is targeting U.S. government relief agencies with disinformation activities that would set the U.S. government on a collision course with citizens who would lose confidence in their competence to manage disaster relief efforts (U.S. Department of Homeland Security, 2024). According to the U.S. Government Accountability Office (2024), disinformation is both an avenue to stifle dissent and promote China. Some of the disinformation strategies that China employs are "propaganda and censorship", monitoring and dictating information dissemination on China's internet platforms, taking advantage of their memberships of international bodies and agreements with other countries, using world renowned figures to advance their agenda, and dictating the activities of "Chinese language media" (GAO, 2024).

Russia

The Internet Research Agency (IRA) is credited with responsibility for Russia's sustained disinformation actions against the United States and its interests (Hicks, *et al.*, 2019; MacFarquhar, 2018). Russia spreads disinformation through the communication machinery of the Russian government, government-backed channels such as RT and Sputnik, tactical use of social media, cloning of websites, and stealthily supporting individuals and institutions to develop internet platforms (GAO, 2024).

Iran

Iran has scaled up information-related operations against its adversaries in the Middle East and the United States (Stubbs & Bing, 2018; Eisenstadt, 2017). The United States has revealed Iran's use of cyber activities to conduct intelligence operations (Hicks, *et al.,* 2019). Information actions led by the Iranian government are undertaken to enhance the country's status as a force in the Middle East

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

and to position it as a direct adversary to Saudi Arabia and Israel (Eisenstadt, 2017). According to Hicks *et al.*, (2019), Iran has interfered with transmissions of major Western media outlets like the British Broadcasting Corporation and the Voice of America as a countermeasure whenever they are faced with unfavorable situations both at home and abroad.

INFORMATION OPERATIONS AND DISINFORMATION

This is one of the instruments used by adversaries in the Gray Zone to negatively influence a nation's psyche by promoting division and divisive discourse, societal defiance, and deliberately false narratives against rival countries (Hicks, *et al.*, 2019). Digital platforms are used in this type of Gray Zone activity. Hicks, *et al.*, (2019) further explain that Russia is the most effective in deploying information operations against the United States. China and Iran also adopt this tactic against the United States. According to Hicks et al. (2019), information operations do not require high financial investments; as such, adversaries deploy this scheme in conjunction with their sophisticated online expertise and network to effect disinformation attacks targeting the United States. Information operations are difficult to track and attribute once they breach secure systems. Democratic and legal safeguards on civil liberties and freedom of speech pose a conundrum on monitoring these platforms and avenues of disinformation (Hicks, *et al.*, 2019) spread without infringing on the rights of citizens.

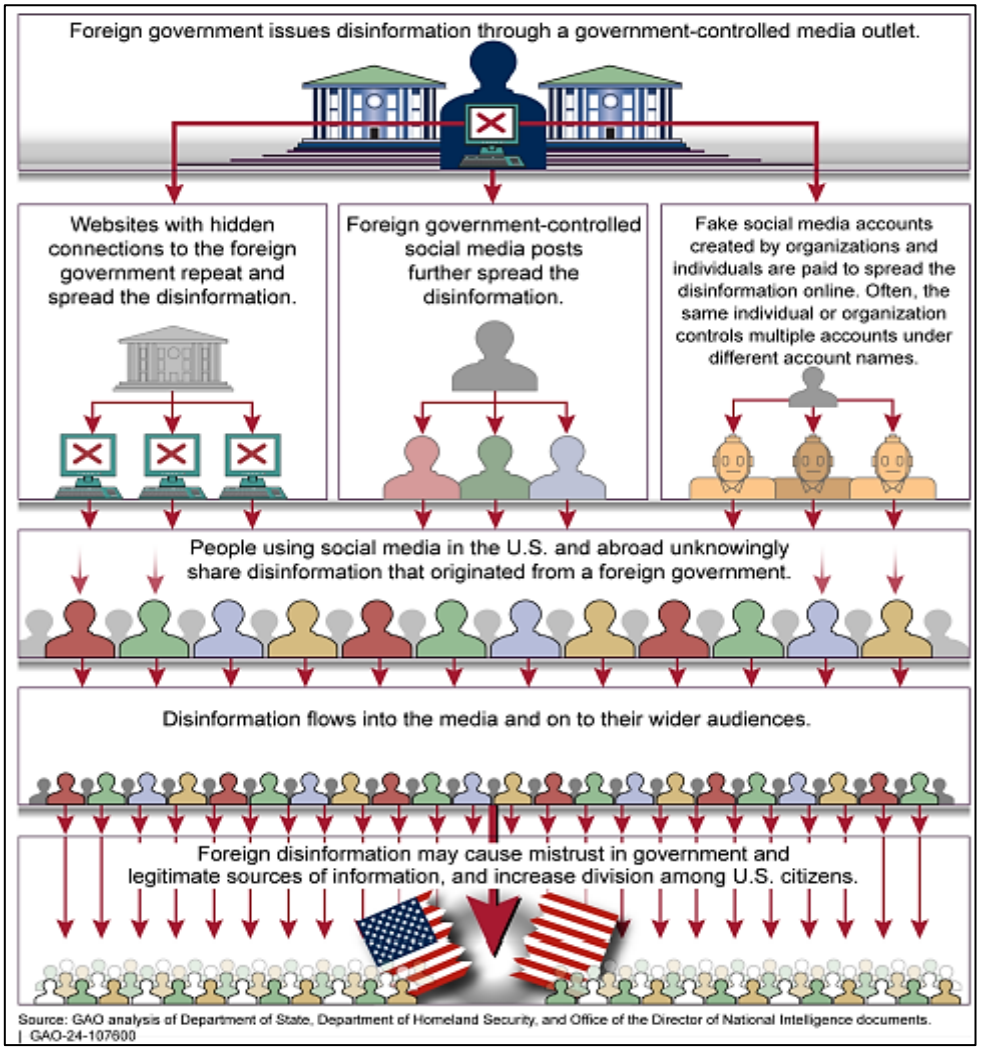


Figure 2: shows one strategy that foreign adversaries deploy to execute information operations (disinformation) against another country (U.S. Government Accountability Office, 2024).

AGENCY RESPONSES TO THREATS

An enhanced appreciation of the information environment demands a committed approach to rigorous examination of pertinent operators and their targets, and a recognition of various strategies used by adversaries (Heap, Hansen, & Gill, 2019).

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

The Foreign Malign Influence Center (FMIC) was established by Congress in 2019 as an organization responsible for evaluating information on foreign threats and assisting in countermeasures against the United States' enemies posing dangers to the United States and its interests (DeVine, 2024). The FMIC is at the forefront of addressing foreign malign influence issues from rival countries. They are tasked with alerting the intelligence community of malign influence activity (DeVine, 2024). According to the Office of the Director of National Intelligence (n.d.), the FMIC is in charge of gathering and examining materials available to the Intelligence Community (IC) and determining deficiencies in these materials. The FMIC also collaborates with the private sector and non-governmental institutions, including civil society organizations. The Center integrates opinions from experts across the broad spectrum of the Intelligence Community (IC) to provide tactical evaluation on what America's enemies plan to do, how they are going to do it, and their resource base to advance their agendas against the United States Office of the Director of National Intelligence (n.d.).

Under the Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency (CISA) and the Office of Intelligence and Analysis (I&A) address disinformation operations from foreign entities. CISA is involved in public sensitization in collaboration with state officials on election-related disinformation campaigns. CISA's primary interest is in disinformation actions that target America's election system (U.S. Government Accountability Office, 2024).

The Office of Intelligence and Analysis (I&A) evaluates dangers posed to the United States. They are responsible for detecting disinformation actions and notifying officials at all levels in the United States (U.S. GAO, 2024). They find FMI operators who use false American online identities, gather information about their actions, evaluate this information, and distribute it to interested parties (U.S. GAO, 2024).

At the Department of Defense, senior officers are responsible for formulating policy and determining the approach to dealing with information-related foreign malign influence. In addition, Public Affairs releases statements across the media (including social media) with accurate information as a countermeasure to disinformation attacks (U.S. GAO, 2024). The Department of Defense has "combatant commands" that identify and counteract disinformation from foreign actors. These "combatant commands" comprise the U.S. Cyber Command, the U.S. Northern Command, and the U.S. European Command. They are each tasked with countering a unique set of disinformation operations from different adversaries with separate instructions and operational parameters (U.S. GAO, 2024).

Table 1: indicates the National Intelligence Council's effort to streamline what constitutes information-related foreign malign influence for U.S. government agencies (U.S. GAO, 2024).

The National Intelligence Council publishes these in their *IC Lexicon for Foreign Malign Influence*	
Term	**Definition**
Foreign Malign Influence	Subversive, undeclared (including covert and clandestine), coercive or criminal activities by foreign governments, non-state actors, or their proxies to affect another nation's popular or political attributes, perceptions, or behaviors to advance their interests.
Disinformation	False or misleading information deliberately created or spread with the intent to deceive or mislead.
Misinformation	False, inaccurate, or misleading information that is spread regardless of the intent to deceive. An adversary's intent can change misinformation to disinformation.
Propaganda	True, partially true, or false information intended to advance an actor's interests by influencing the attitudes, perceptions, or behaviors of an audience. Propaganda could be intended to influence the creator's domestic audience or aimed at a foreign audience.

Source: National Intelligence Council Memorandum 2022-17680, *Updated IC Lexicon for Foreign Malign Influence* (August 19, 2022) | GAO-24-107600

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

Effective collaboration between government agencies and private corporations led to the uncovering and termination of several Facebook and Instagram accounts engaged in information-related foreign malign influence (Gleicher, 2020).

Implementation Challenges

Notwithstanding the efforts made by government agencies with some private sector support, efforts are plagued with some drawbacks, which have prevented effective suppression of disinformation activities from America's rivals.

One of the challenges that plagues the effective utilization of strategic communications to address foreign disinformation is the lack of a harmonized strategy across government agencies. The Departments of Defense and Homeland Security have different agencies working to address disinformation challenges to the United States. But without collaboration across agencies and departments, there may be duplication of functions and personnel without effectively addressing foreign disinformation actions.

Issues arise in addressing information operations in foreign malign influence with regard to the likelihood that measures to curb disinformation encroach on First Amendment rights (Library of Congress & Law Library of Congress, n.d.). Even though disinformation in this context refers to foreign actors, in cases where citizens are used for these operations, upholding their First Amendment rights while protecting the republic from these malign activities becomes a contentious issue.

The strategic communications framework is unable to adequately match the rate of technological advancements. Rivals of the United States are taking advantage of the rapid pace of developments in AI and its cost-effectiveness to enhance their network and improve the obscurity of their operations. Brundage et al. (2020) note that U.S. government agencies are constrained financially, in terms of technical infrastructure and the human expertise to quickly detect information operations threats as soon as they emerge.

Governmental responses are subject to the ideology of the administering political authority. With strategies heavily influenced by political leanings, there are inconsistencies in approach from a strategic communications perspective and this affects the achievement of a unified strategy against foreign disinformation. The Global Engagement Center was established to directly deal with disinformation from foreign adversaries of the United States (U.S. Department of State, n.d.). The absence of bipartisan support and complaints of First Amendment infringements led to the shutdown of the Center at the end of 2024 (Weed, 2024).

RECOMMENDATIONS

According to Hicks *et al.*, (2019), there is a need to converge all gray zone activity under one centralized authority to guide policy and strategy among various stakeholders. This will give the central authority a broad view of the threat landscape and allow for a more proactive approach to policymaking, instead of strategy and policy being fragmented in agencies and deployed as a reactionary measure to attacks.

It is essential for private participation in shaping the development of national security policymaking to address threats. Private participation will enhance capacity because of the varied expertise from different sectors that would contribute to policy formulation and support national security and he foreign service in areas where they are technically handicapped (Hicks et. al, 2019).

Systems must be designed to help agencies and personnel assemble large volumes of information from different sources and agencies. With this harmonized gathering point, stakeholders can reach a consensus on measures to address information operations and disinformation attacks from rivals (Hicks *et al*., 2019).

Europe has made significant strides that the United States can emulate in countering disinformation. The Digital Services Act (DSA) is a regulation that aims to protect citizens by making the online environment safe for individuals (European Parliament & Council, 2022).

Europe has adopted an elaborate regulatory framework to curb disinformation. The Digital Services Act is a regulation that aims to protect citizens by making the online environment safe for individuals (European Parliament & Council, 2022). The European Union's (EU) Code of Conduct for Disinformation is pivotal to the EU's approach against disinformation. Stakeholders (including platform owners) participated in the establishment of the Code and signed to uphold it and use it as a guide for their operations. The DSA involved clear content policy disclosure measures, obligatory safety appraisals, and algorithm evaluation for major platforms (European Parliament & Council, 2022). The United States can draw lessons from Europe's experience by

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

analyzing its enforcement challenges, lopsided financial constraints that benefit large-scale platforms, and Europe's handling of free speech concerns.

The EU's measures allow for collaboration to enforce regulations where online giants like Google, TikTok, and Meta monitor content on their platforms, apply sanctions, and exercise responsibility in the disclosure of these online activities and their responses to them.

The United States can emulate the inclusive approach, which incorporates the input of a cross-section of society and relevant players to garner the support of all these stakeholders. Also, to douse free speech encroachment tensions, this approach could be effective as it would factor First Amendment infringement concerns into a regulation that encapsulates America's unique experiences with foreign malign influence in the information operations and disinformation.

Finland success in tackling disinformation can be attributed to its National Security Strategy which adopted a "whole-of-society" blueprint incorporating citizen sensitization, media literacy education and the collaboration of stakeholders from a wide range of industries (Prime Minister's Office, 2017). Strategies for countering foreign influence must be holistic and must tackle both threats from foreign adversaries and susceptibilities within the U.S. that magnify narratives of division and this demands consistent teamwork through governmental and non-governmental agencies (Nabila & Thompson, 2025). In addition, by making media literacy a key component of the Finnish educational system (Cord, 2022), citizens grow up informed and critical of the information they are exposed to, thereby reducing their likelihood of becoming victims of disinformation.

CONCLUSION

The United States continues to grapple with foreign influence operations from China, Russia and, Iran. However, with frequent and non-uniform responses to these threats, and technological gaps, adversaries are still able to execute successful information-related foreign influence operations targeting societal harmony and democratic institutions. Strategic communications is pivotal to national security policy in countering information operations and the disinformation aspect of foreign influence. For it to be an effective strategy, it must be responsive to the rate of technological advancement and must draw from the experience and expertise of the best minds across various sectors. The United States can draw from successes in Europe, where every segment of society contributes to the design and implementation of strategies that ultimately work for them. This is an essential part of stifling information operations and disinformation. Concerns about free speech infringements can be addressed if the is a broad acknowledgement of the dangers posed by disinformation, coupled with a commitment to develop effective bipartisan solutions which would outlive political administrations and serve as a path way to achieving societal cohesion. Effective strategic communications frameworks are central to the protection of democratic institutions and national security against foreign influence threats.

REFERENCES

1. Bolt, N., ed. *Defence Strategic Communications*. Vol. 6 (Spring 2019). NATO Strategic Communications Centre of Excellence, 2019. https://stratcomcoe.org/cuploads/pfiles/web_academic_journal_volume_6.pdf. DOI: 10.30966/2018.RIGA.6.
2. Fridman, O. "Defining Foreign Influence and Interference." *INSS Special Publication* (2024): 1–12. https://kclpure.kcl.ac.uk/ws/portalfiles/portal/242820492/Defining_Foreign_Influence_and_Interference.pdf.
3. Cybersecurity and Infrastructure Security Agency. *Foreign Influence Taxonomy*. Publication No. 19_0717. U.S. Department of Homeland Security, July 17, 2019. https://www.cisa.gov/sites/default/files/publications/19_0717_cisa_foreign-influence-taxonomy.pdf.
4. Nabila, M. H., and M. Thompson. "The Impact of Disinformation on National Security Policymaking: A Review." *EPRA International Journal of Multidisciplinary Research* 11.6 (2025): 1891–1899. https://doi.org/10.36713/epra22781.
5. U.S. Department of Justice Office of the Inspector General. *Evaluation of the U.S. Department of Justice's Efforts to Coordinate Information Sharing about Foreign Malign Influence Threats to U.S. Elections*. Report No. 24-080. July 2024. https://www.oig.justice.gov/sites/default/files/reports/24-080.pdf.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

6. Bolt, N. "Foreword." *Defence Strategic Communications* 6 (2019): 4–5. NATO Strategic Communications Centre of Excellence. https://doi.org/10.30966/2018.RIGA.6.
7. Althuis, J. "How U.S. Government Fell in and out of Love with Strategic Communications." *Defence Strategic Communications* 10 (2021): 71–110. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/how-us-government-fell-in-and-out-of-love-with-strategic-communications/226.
8. Office of the Director of National Intelligence. *The Foreign Malign Influence Center*. n.d. Retrieved July 28, 2025. https://www.dni.gov/index.php/fmic.
9. Byman, D. "Foreign Malign Influence Targeting U.S. and Allied Corporations." *Center for Strategic and International Studies* (Policy Brief, March 20, 2025). https://www.csis.org/analysis/foreign-malign-influence-targeting-us-and-allied-corporations.
10. Federal Bureau of Investigation. *Foreign Malign Influence and Higher Education*. Background Briefing. U.S. Department of Justice, October 18, 2024. https://www.fbi.gov/file-repository/reports-and-publications/foreign-malign-influence-and-higher-education-101824.pdf
11. Kahler, M. *Foreign Influence and Democratic Governance: Defining and Countering Malign Influence*. Council Special Report. Council on Foreign Relations, Oct. 2024. https://www.cfr.org/report/foreign-influence-and-democratic-governance.
12. Hicks, K. H., M. Dalton, M. Donahoe, L. R. Sheppard, A. H. Friend, M. Matlaga, J. Federici, M. Conklin, and J. Kiernan. *By Other Means Part II: U.S. Priorities in the Gray Zone*. Center for Strategic and International Studies, Aug. 2019. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/Hicks_GrayZone_II_full_WEB_0.pdf.
13. Morris, L. J., M. J. Mazarr, J. W. Hornung, S. Pezard, A. Binnendijk, and M. Kepe. *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression below the Threshold of Major War*. RAND Corporation, 2019, pp. 7–8. https://www.rand.org/pubs/research_reports/RR2942.html.
14. U.S. Department of Homeland Security, Office of Intelligence & Analysis. *Homeland Threat Assessment 2025*. Publication 24-320-IA. Sept. 30, 2024. https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf.
15. Hicks, K. H., A. H. Friend, J. Federici, H. Shah, M. Donahoe, M. Conklin, A. Akca, M. Matlaga, and L. Sheppard. *By Other Means: Part I — Gaining Competitive Advantage in the Gray Zone*. Center for Strategic and International Studies, 2019. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/Hicks_GrayZone_interior_v4_FULL_WEB_0.pdf.
16. MacFarquhar, N. "Inside a Russian Troll Factory: Kremlin's Covert Campaign to Sow U.S. Discord." *The New York Times*. Feb. 18, 2018. https://www.nytimes.com/2018/02/18/world/europe/russia-troll-factory.html.
17. Stubbs, J., and C. Bing. "Special Report: How Iran Spreads Disinformation around the World." *Reuters*. Dec. 1, 2018. https://www.reuters.com/article/world/special-report-how-iran-spreads-disinformation-around-the-world-idUSKCN1NZ1FE/.
18. Eisenstadt, M. "Information Warfare: Centerpiece of Iran's Way of War." In K. H. Hicks and M. G. Dalton, eds. *Deterring Iran after the Nuclear Deal*, 75–86. Center for Strategic and International Studies (CSIS), 2017. https://www.jstor.org/stable/resrep23152.12.
19. U.S. Government Accountability Office. *Foreign Disinformation: Defining and Detecting Threats*. GAO-24-107600. Sept. 26, 2024. https://www.gao.gov/assets/gao-24-107600.pdf.
20. DeVine, M. E. *The Intelligence Community's Foreign Malign Influence Center*. CRS In Focus No. IF12470. Congressional Research Service, Nov. 27, 2024. https://sgp.fas.org/crs/intel/IF12470.pdf.
21. Heap, B., ed., P. Hansen, and M. Gill. *Strategic Communications Hybrid Threats Toolkit: Applying the Principles of NATO Strategic Communications to Understand and Counter Grey Zone Threats*. NATO Strategic Communications Centre of Excellence, 2019. https://stratcomcoe.org/publications/download/Strategic-Communications-Hybrid-Threats-Toolkit.pdf.
22. Office of the Director of National Intelligence. *What We Do*. n.d. Retrieved July 21, 2025.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

https://www.dni.gov/index.php/fmic/what-we-do.
23. Gleicher, N. "Removing Coordinated Inauthentic Behavior." *Meta Newsroom Post*. Sept. 24, 2020. https://about.fb.com/news/2020/09/removing-coordinated-inauthentic-behavior-russia/.
24. Library of Congress & Law Library of Congress. *First Amendment: Freedom of Religion, Speech, Press, Assembly, and Petition.* In *The Constitution Annotated*. n.d. Retrieved July 29, 2025. https://constitution.congress.gov/constitution/amendment-1/.
25. Brundage, M., S. Avin, J. Wang, H. Belfield, G. Krueger, G. Hadfield, H. Khlaaf, J. Yang, H. Toner, R. Fong, T. Maharaj, P. W. Koh, S. Hooker, J. Leung, A. Trask, E. Bluemke, J. Lebensold, C. O'Keefe, M. Koren, … M. Anderljung. *Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims*. arXiv, 2020. https://arxiv.org/abs/2004.07213.
26. U.S. Department of State. *About Us – Global Engagement Center*. n.d. Retrieved July 29, 2025. https://2021-2025.state.gov/about-us-global-engagement-center-2/.
27. Weed, M. C. *Termination of the State Department's Global Engagement Center*. CRS Insight No. IN12475. Congressional Research Service, Dec. 26, 2024. https://crsreports.congress.gov/product/pdf/IN/IN12475.
28. European Parliament & Council of the European Union. *Regulation (EU) 2022/2065 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act). Official Journal of the European Union* L 277 (Oct. 19, 2022): 1–102. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065.
29. European Commission. *Code of Conduct on Disinformation.* EU Digital Strategy, Feb. 13, 2025. https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation.
30. Prime Minister's Office. *Government Defence Report to Parliament: The Government's Defence Policy Report 2017*. Publication 7/2017. Government of Finland, Feb. 16, 2017. https://www.defmin.fi/files/3688/J07_2017_Governments_Defence_Report_Eng_PLM_160217.pdf.
31. Cord, D. J. "Educated Decisions: Finnish Media Literacy Deters Disinformation." *Finland.fi*. June 2022. https://finland.fi/life-society/educated-decisions-finnish-media-literacy-deters-disinformation/

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Nabila, M. H. and Thompson, M." Countering Foreign Influence: The Role of Strategic Communications in National Security Policy Making in the United States." *Sarcouncil journal of Arts humanities and social sciences* 4.9 (2025): pp 22-30.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher