U.S. Government Accountability Office

FOREIGN DISINFORMATION: Defining and Detecting Threats

GAO-24-107600
Q&A Report to Congressional Requesters
September 26, 2024

Why This Matters

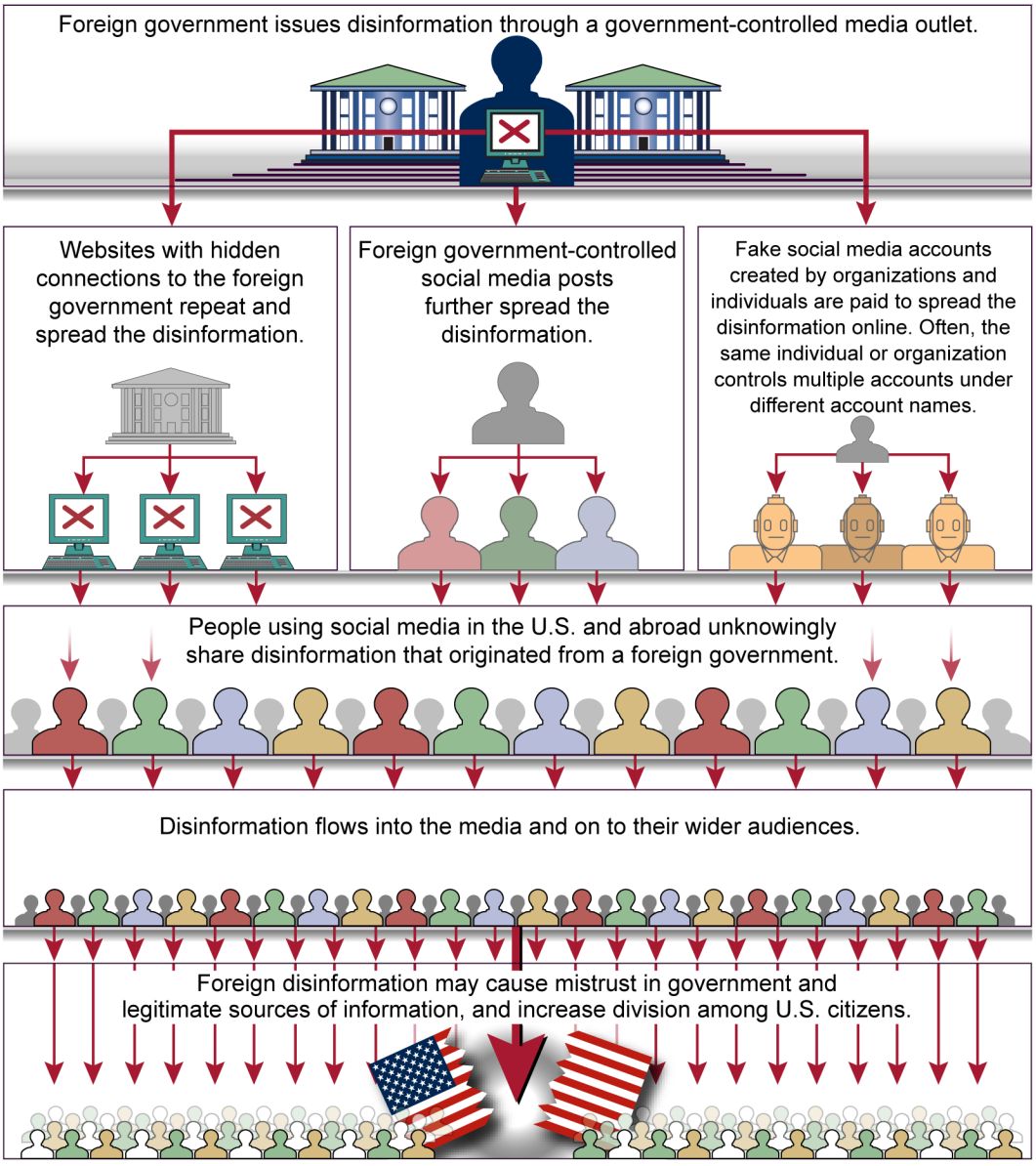
Foreign disinformation—defined in this report as false claims or misleading information deliberately created or spread by foreign actors to deceive people—threatens U.S. national security. Disinformation can weaken democracies while increasing political instability and conflict among people, according to reports from the Office of the Director of National Intelligence (ODNI). Foreign disinformation is a type of foreign malign influence activity. Tactics to create or spread disinformation include employing foreign actors behind fake social media accounts and using websites with both hidden operators and hidden connections to foreign governments.

U.S. agencies have reported that foreign governments have conducted disinformation campaigns in recent years to undermine U.S. foreign policy interests and disrupt civil discussions in the United States and abroad. These foreign governments spread disinformation in a variety of ways, including through state-run or sponsored propaganda, social media, and artificial intelligence—such as deepfakes, which are videos, photos, or audio recordings that appear real but have been manipulated with artificial intelligence.

U.S. federal agencies that conduct activities to counter disinformation spread by foreign actors include the Departments of State (State), Homeland Security (DHS), and Defense (DOD).

In recent years, ODNI, State, and DHS have reported that foreign governments, terrorists, and extremist groups spread disinformation to gain influence. Once disinformation is released, it can spread very rapidly as individuals and media outlets share the narratives as shown in figure 1.

Figure 1: How Might Foreign Governments Quickly Spread Disinformation?



Source: GAO analysis of Department of State, Department of Homeland Security, and Office of the Director of National Intelligence documents. | GAO-24-107600

Note: The graphic above depicts one example among many possible ways of how foreign governments might spread disinformation.

We were asked to describe U.S. efforts to counter foreign disinformation. This first of two reports examines how relevant U.S. government agencies define and detect foreign disinformation threats and the legal authorities these agencies use to counter these threats. U.S. agencies counter foreign disinformation created or spread by both foreign governments and non-state actors, such as terrorist groups. However, because many of these agencies' efforts focus on foreign governments, this report primarily discusses foreign governments that spread disinformation rather than non-state actors.

Recent reports have raised questions about whether the federal government has a clear lead agency to coordinate efforts to counter foreign disinformation and whether existing coordination mechanisms are mature. In our second report, we plan to examine these and other issues by evaluating U.S. agency efforts to

share information and coordinate their actions to counter foreign disinformation. We plan to issue this second report in 2025.

Key Takeaways

- State, DHS's Office of Intelligence of Analysis (I&A), and DOD monitor both public and nonpublic sources of information and use a variety of methods to detect foreign disinformation targeted at overseas or domestic audiences, depending on the agency. For example, State and DHS's I&A analyze social media to identify disinformation and disinformation actors.
- State, DHS, and DOD conduct activities to counter foreign disinformation targeted at audiences overseas or domestically, depending on the agency. Collectively, these activities include identifying, publicizing, and researching disinformation threats as well as educating U.S. and foreign partners and the public on how to recognize and build resilience against disinformation threats.
- To define foreign disinformation and related terms, most of the U.S. agencies we spoke to use the National Intelligence Council's *IC Lexicon for Foreign Malign Influence,* which aims to standardize terms and add precision to disinformation analysis.

What are the main foreign governments that create and spread disinformation?

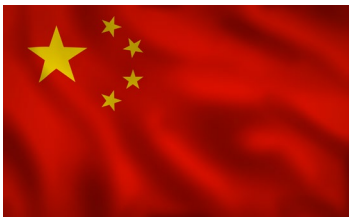
In recent years, the main foreign governments that have been creating and spreading disinformation are the Russian Federation (Russia), the People's Republic of China (PRC), and the Islamic Republic of Iran (Iran), according to State, DHS, the Department of Justice, and ODNI officials. ODNI's Foreign Malign Influence Center's (FMIC) statutory functions include providing federal employees and officers in policy-making positions as well as Congress with comprehensive assessments, indications, and warnings of the threat of foreign malign influence campaigns from these three countries.[1]

U.S. agencies reported that generally, these foreign governments spread disinformation to gain influence and promote their viewpoints globally.

Russia has been actively creating and spreading disinformation on numerous subjects, including the Ukraine conflict, to targeted audiences throughout the world, according to State's Global Engagement Center (GEC). State's GEC identified five primary methods that Russia uses to spread disinformation, including (1) official government communications, (2) state-funded global messaging such as *RT* and *Sputnik*, (3) weaponization of social media, (4) cyber-enabled techniques like "spoofed" websites intending to impersonate legitimate websites, and (5) websites maintained by organizations or individuals who may have secret connections to Russia. For example:

- Russia attempted to undermine global support for Ukraine by providing pro-Russia disinformation to local media contacts in Latin America, who then published the information as if it had originated locally, according to State.[2] Russia has also likely backed websites, such as *DC Weekly*, that impersonate U.S. news websites and push Russian government propaganda while also reporting on local news, culture, and politics to make their websites appear as credible sources, according to researchers and DHS officials.
- Clemson University's *Media Forensics* Hub reported that posts from *DC Weekly* have falsely claimed Ukrainian President Volodymyr Zelensky and his wife were improperly using foreign aid to enrich themselves. For example, a

November 2023 article from *DC Weekly* falsely claimed Zelensky had used American aid money to buy two yachts.



The People's Republic of China (PRC) has also actively been creating and spreading disinformation globally to boost pro-PRC content and suppress criticism. GEC reports that PRC's approach features five primary methods: (1) leveraging propaganda and censorship, (2) promoting PRC surveillance technology, information control tactics, and norms for governing digital platforms favorable to PRC's preferences, (3) exploiting international organization and bilateral partnerships, (4) co-opting—fostering mutually advantageous relationships with—and pressuring prominent individuals to shape their views in line with PRC's desired narratives, and (5) exercising control of Chinese-language media, such as *China Media Group, People's Daily,* and *Xinhua.*[3]

For example, GEC reported that PRC employs:

- software applications that run automated tasks on the Internet, usually with the intent to imitate human activity such as messaging on a large scale—these are known as bots.
- individuals who post messages online with the intention of distracting from an online discussion or causing fear and anger—these are known as internet trolls. Trolls that hide their true identities or origins may be part of a disinformation operation or campaign.
- fake social media accounts and "flooding," a tactic that manipulates search engine results and hashtag searches. GEC reported that PRC has used flooding to drown out information around sensitive topics with unrelated content that renders fact-based, substantive information more difficult for users to find.
- In a specific example, PRC used social media channels and traditional state-controlled media to disseminate and amplify false claims in Zimbabwe to promote Chinese political and business propaganda and push anti-Western narratives, according to DOD's Africa Center for Strategic Studies.[4]

Iran is becoming increasingly aggressive in its efforts to pass on disinformation to stoke conflict and undermine confidence in U.S. democratic institutions, according to ODNI.[5] Iran uses social media platforms, Iran-based online influencers, and state-controlled media to spread disinformation. For example, the U.S. Agency for Global Media reported that Iran's state-controlled *Press TV* in English and French, and *HispanTV* in Spanish both target foreign audiences to promote narratives from the viewpoint of Iranian government leaders.

What are the main agencies that conduct activities to counter foreign disinformation threats?

As represented in figure 2, U.S. federal entities, including within State, DHS, and DOD, conduct activities to counter foreign disinformation. Collectively, these activities include identifying disinformation threats, publicizing disinformation threats, researching and analyzing disinformation threats, and educating the U.S. and foreign partners and the public on how to recognize disinformation threats and build resilience against them. We have issued several reports on disinformation.[6]

Figure 2: U.S. Federal Entities that Conduct Activities to Counter Foreign Disinformation

Source: Semper Fidelis/stock.adobe.com. | GAO-24-107600

Agencies' responsibilities to counter foreign disinformation vary. Some U.S. entities' primary mission, for example, GEC, is to counter foreign disinformation overseas while officials from other U.S. entities, such as DOD's combatant commands, said these efforts support their broader missions. State officials told us that the department is also engaged in an array of training and capacity building programs to help improve the public's ability to identify and resist foreign disinformation.

In addition, some intelligence and law enforcement entities, such as the FBI, conduct activities to counter foreign malign influence activities.[7] The National Intelligence Council defines foreign malign influence activities as 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.

For example, FMIC's function is to serve as the U.S. government's primary organization for analyzing and integrating all intelligence the U.S. government has possessed or acquired pertaining to foreign malign influence, among other things.[8] FMIC's Election Threats Executive leads the intelligence community's efforts to identify and assess foreign malign influence and interference in U.S. elections.

State, DHS, and DOD officials told us they do not counter the actions of U.S. citizens who create or spread disinformation. Instead, these agencies either focus on countering disinformation threats that have a foreign origin, or they broadly distribute accurate information to educate the public, set the record straight, or build resilience to disinformation.

What is the role of the Department of State to counter foreign disinformation?

State Department entities that are involved in efforts to counter foreign disinformation include the GEC and the Under Secretary for Public Diplomacy and Public Affairs. In addition, the Bureau of Intelligence and Research (INR) assesses the susceptibility of foreign target audiences to disinformation.

Global Engagement Center

GEC's statutory purpose is to direct, lead, synchronize, integrate, and coordinate efforts of the federal government to recognize, understand, expose, and counter foreign state and foreign non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the U.S. and U.S. allies and partner nations.[9] GEC officials said that they focus on disinformation that originates abroad and is targeted at foreign audiences. According to GEC officials, their work focuses on:

- Helping U.S. federal agencies, international partners, and U.S. embassies develop analytic skills, policy responses, and technical capacity to counter foreign disinformation overseas. This includes sharing technologies and techniques with U.S. and foreign partners to counter foreign disinformation.
- Using public communication platforms to expose foreign disinformation, such as published products, social media posts, and press releases. For example, GEC issued a report on the PRC's global disinformation efforts and exposed the Islamic State of Iraq and Syria (ISIS) propaganda by informing the public via radio programming in West Africa.
- Advancing and facilitating the use of data and innovative technologies to improve the U.S. and its partners' abilities to counter foreign disinformation.

In addition to these activities, GEC's Counterterrorism division exposes and counters terrorist propaganda that seeks to exploit audience vulnerabilities, create instability that weakens democratic governments, and build support for networks to carry out terrorist attacks, according to GEC officials.

Under Secretary for Public Diplomacy and Public Affairs

State's Public Diplomacy sections at U.S. embassies abroad detect, report on, and counter disinformation emerging in host countries. For example, a State official said that U.S. Embassy staff in Zimbabwe monitor PRC disinformation in the region.

Bureau of Intelligence and Research

INR officials told us they do not counter disinformation, but instead assess the susceptibility of foreign target audiences to disinformation. INR researches and analyzes information detected from other entities, publishes reports based on its analysis, and disseminates them widely within State and the intelligence community.

What is the role of the Department of Homeland Security to counter foreign disinformation?

Two entities within the DHS are primarily involved in efforts to counter foreign disinformation. These entities are the Cybersecurity and Infrastructure Security Agency (CISA) and the Office of Intelligence and Analysis (I&A).

Cybersecurity and Infrastructure Security Agency

Among its other duties to manage and reduce risk to U.S. cyber and physical infrastructure, CISA officials told us that CISA's current work to address the risk posed by foreign influence operations and disinformation is focused on election infrastructure. According to these officials, CISA educates the public on the risks of disinformation and partners with state and local election officials to disseminate educational materials to help them identify disinformation. For example, CISA has published guidance and numerous fact sheets, such as *Tactics of Disinformation* that highlight disinformation threats as well as educate the public on the steps they can take to increase their resilience to disinformation.[10]

CISA officials told us they do not distinguish between disinformation threats originating in the U.S. or abroad because they focus on building resilience to foreign malign influence operations to reduce risks to U.S. election infrastructure.

Office of Intelligence and Analysis

I&A is DHS's primary intelligence office that works to identify and analyze threats against the homeland. I&A officials told us they identify disinformation threats and disseminate this information to federal, state, local, tribal, and territorial officials. I&A focuses on identifying foreign malign influence actors who spread disinformation on behalf of a foreign government, including through fake American online personas.[11] I&A collects messaging disseminated by these actors, and produces assessments of these actors' targets, tactics, and procedures. They then share these assessments with relevant stakeholders and partners. For example, in 2023, I&A published an assessment of Chinese municipal authority accounts' amplification of Beijing state media propaganda.

What is the role of the Department of Defense to counter foreign disinformation?[12]

Several entities within the DOD are involved in creating policy and conducting activities to counter foreign disinformation. These entities include officials and offices from within the Office of the Secretary of Defense (OSD), and DOD's combatant commands.

Office of the Secretary of Defense

According to DOD officials, OSD senior department officials and their offices develop policy, guidance, and strategy, including on information operations. These officials and offices include

- The Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict's Office of Information Operations Policy,
- The Assistant Secretary of Defense for Cyber Policy (also serves as the DOD Principal Cyber Advisor), and
- The Assistant to the Secretary of Defense for Public Affairs.

In addition, Public Affairs publishes statements, messages on social media, and press releases with factual information to counter disinformation.

Combatant Commands

DOD's combatant commands focus on achieving national security objectives and protecting U.S. national interests. Combatant commands can utilize and integrate air, land, sea, and amphibious forces within a specific geographic area (for example, U.S. Northern Command) or can operate worldwide using a specific capability (for example, U.S. Cyber Command). DOD's combatant commands detect and counter disinformation, but the scale and scope of their activities vary by command, according to DOD officials, For example:

- The U.S. European Command counters Russian disinformation regarding the war in Ukraine while the U.S. Africa Command counters disinformation spread by PRC throughout the region.
- U.S. Northern Command is most concerned with disinformation that may undermine U.S. public trust of U.S. military activities.
- U.S. Cyber Command regularly observes and disrupts foreign malicious cyber activities supporting the creation and spread of foreign disinformation.

How do these agencies define foreign disinformation threats?

Of the U.S. agencies working to counter foreign disinformation that we spoke to, most use the 34 terms and definitions provided by the National Intelligence Council in the *Updated IC Lexicon for Foreign Malign Influence* (IC Lexicon) to define foreign disinformation threats.[13] The council originally published the IC Lexicon in April 2021 and updated it in August 2022. The updated IC Lexicon states that it is intended to standardize the terms intelligence community agencies use to describe foreign malign influence activities, and to add precision to these agencies' analyses. Table 1 provides a sample of foreign malign influence terms from the IC Lexicon.

Table 1: Examples of the National Intelligence Council Terms and Definitions Related to Foreign Malign Influence

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

Note: According to DHS/CISA officials, CISA does not follow the IC Lexicon for Foreign Malign Influence but uses its own definitions. For example, CISA uses the following definition for disinformation: "Disinformation is deliberately created to mislead, harm, manipulate a person, social group, organization, or country." See https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation

DHS officials told us that while the IC Lexicon provides common definitions that most intelligence agencies use, these definitions may differ from those contained in existing legal authorities or policies. For example, the definition of foreign malign influence contained in the IC Lexicon differs from the definition outlined in FMIC's legal authority.[14]

What legal authorities do these agencies use to counter foreign disinformation threats?

As illustrated in table 2, State, DHS, and DOD identified various legal authorities they use to counter foreign disinformation. Some entities, like GEC, have specific legal authorities outlining actions to counter foreign disinformation. Conversely, other entities do not have specific legal authorities related to disinformation, but engage in activities to counter disinformation as part of their broader mission.

Table 2: Selected U.S. Agency-Identified Legal Authorities Used to Counter Foreign Disinformation

U.S. Agency and Office	Legal Authority Identified
State Department's Global Engagement Center (GEC)	National Defense Authorization Act for Fiscal Year 2017 (FY17 NDAA) as amended by John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY19 NDAA) directs GEC to support the development and dissemination of fact-based narratives and analysis to counter propaganda and disinformation directed at the U.S. and U.S. allies and partner nations, among other things.[a] Executive Order 13721 established GEC and assigned responsibilities for the Center.[b]
State Department's Bureau of Intelligence and Research (INR)	No specific legal authorities to counter foreign disinformation, according to State officials. However, as a member of the intelligence community under Executive Order 12333, as amended, INR is directed to collect, analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions.
State Department's Under Secretary for Public Diplomacy and Public Affairs	22 U.S.C. § 1461(a) authorizes the use of certain funds to provide for the preparation, dissemination, and use of information intended for foreign audiences abroad about the U.S., its people, and its policies, through press, publications, radio, motion pictures, the Internet, and other information media, including social media, and through information centers, instructors, and other direct or indirect means of communication.
Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA)	CISA relies on its statutory authorities and obligations, including those under Title 6 of the U.S. Code and the National Security Memorandum on Critical Infrastructure Security and Resilience, to mitigate risks to the nation's critical infrastructure. Countering disinformation is broadly authorized as part of CISA's mission to protect the homeland against these threats, according to DHS officials.[c]
DHS's Office of Intelligence and Analysis (I&A)	I&A relies on its statutory authorities under the Homeland Security Act of 2002, as amended, codified at 6 U.S.C. § 121(d), as well as the President's direction in Executive Order 12333, as amended, to carry out this mission, according to DHS officials.[d]

Selected Officials and Offices within the Office of the Secretary of Defense: Assistant Secretary of Defense for Cyber Policy; Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict's Office of Information Operations Policy; The Assistant to the Secretary of Defense for Public Affairs	No specific legal authority to counter foreign disinformation, according to DOD officials. However, DOD officials pointed to 10 U.S.C. § 397, which authorized the position of Principal Information Operations Advisor with responsibilities to include overall integration and supervision of the deterrence of, conduct of, and defense against information operations. Agency officials also pointed to a provision in the fiscal year 2023 NDAA that created the position of Assistant Secretary of Defense for Cyber Policy with responsibilities for overall supervision of DOD policy for cyber. This official also serves as the Principal Cyber Adviser, who advises the Secretary of Defense on military cyber forces and activities.[e]
DOD Combatant Commands	10 U.S.C. § 164 provides Combatant Command commanders the authority to conduct operations to accomplish their assigned military mission, according to DOD officials. DOD instruction 3607.02 provides that Combatant Commands will conduct Military Information Support Operations for various reasons, including to counter enemy or adversary information and influence activities focused on foreign audiences that undermine U.S. national security interests. DOD instruction 5400.13 provides that Combatant Commands will conduct Public Affairs activities to assure the trust and confidence of U.S. population, friends and allies, deter and dissuade adversaries, and counter misinformation and disinformation ensuring effective, culturally appropriate information delivery in regional languages according to DOD Instruction 5160.70.

Source: GAO analysis of agency information and legal authorities identified by agency officials. | GAO-24-107600

[a]FY17 NDAA, Pub. L. No. 114–328, Div. A, Title XII, § 1287, 130 Stat. 2000, 2546-8 (Dec. 23, 2016), as amended by FY19 NDAA, Pub. L. No. 115–232, Div. A, Title XII, § 1284, 132 Stat. 1636, 2076-8 (Aug. 13, 2018), codified as amended at 22 U.S.C. § 2656 note, Global Engagement Center.

[b]*Developing an Integrated Global Engagement Center To Support Government-wide Counterterrorism Communications Activities Directed Abroad and Revoking Executive Order 13584*, 81 Fed. Reg. 14685 (March 15, 2016).

[c]6 U.S.C. § 652; National Security Memorandum/NSM–22, *National Security Memorandum on Critical Infrastructure Security and Resilience* (Apr. 30, 2024).

[d]*United States Intelligence Activities,* 48 Fed. Reg. 59941 (Dec. 4, 1981).

[e]James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117–263, § 901, 136 Stat. 2395, 2747-8 (Dec. 23, 2022).

What types of sources do these U.S. agencies use to detect foreign disinformation?

According to State, DHS I&A, and DOD officials, agencies use several sources to detect foreign disinformation. These include publicly available sources, such as social media networks and news media as well as nonpublic information collected by intelligence agencies or foreign governments. See table 3 for a list of sources that U.S. agencies reported they use to detect foreign disinformation.

Table 3: Sources Reported to be Used by Selected U.S. Agencies to Detect Foreign Disinformation

Availability of Source	Public			Public and Non Public		Nonpublic	
Source	**Social Media**	**News Media**	**Official Foreign Government Sources**	**Proxy Sources**	**Cyber-Enabled Sources**	**Foreign Partner Reporting**	**U.S. Intelligence Reporting**
Description	Information from social media. Includes content of posts and associated data.	Information distributed by traditional news media sources.	Information released directly by a foreign government. These may include government statements, quotes by officials, or releases by state-owned media.	Information released by an organization with secret connections to a foreign government. These may include "troll" farms or misleading news sites.[a]	Information gained, modified, or distributed using cyber techniques, such as spoofed websites[b] and hack-and-release operations,[c] among others.	Information about disinformation threats or actors provided to U.S. agencies by allies and partner nations.	Information gathered and reported by the U.S. intelligence community identifying a disinformation threat or actor.

Source: GAO review of Department of State, Department of Defense, and Department of Homeland Security Intelligence and Analysis documents and interviews. | GAO-24-107600

[a]An internet troll is a person who tries to provoke disputes or create division online. Trolls that hide their true identities or origins may be part of a foreign influence operation or campaign. A troll farm is an entity employing multiple trolls to conduct coordinated disinformation activities on the internet.

[b]Spoofed websites are intended to impersonate legitimate websites by slightly altering web addresses to confuse readers. For example, a disinformation actor may create a fake ".com" version of a legitimate ".gov" website.

[c]Hack-and-release operations involve gaining access to secret or sensitive materials and releasing them publicly to influence policy or opinion.

What types of methods do these U.S. agencies use to detect foreign disinformation?

State, I&A, and DOD employ a variety of methods to detect and analyze foreign disinformation identified through their sources. These include computerized analyses of social media networks, linguistic and regional expert analyses, and assessing foreign media narratives.

Social media analysis. State, I&A, and DOD officials told us they monitor or analyze social media in some form to detect foreign disinformation. When analyzing social media posts for foreign disinformation, these agencies may assess the posts' content and associated data such as location or timestamps.[15]

I&A and GEC officials said they can analyze social media content by filtering for certain words or phrases, searching for inconsistencies in profile information, and looking for evidence of nonhuman behavior. For example, if identical content is reposted multiple times by multiple accounts in a few nanoseconds, this could indicate bot activity possibly tied to a foreign disinformation actor, according to I&A officials.

Other potential indications of foreign disinformation actors include social media profile information that does not match the account's Internet Protocol (IP) address, such as a student who claims to be from Des Moines, Iowa, with an IP address in China, according to I&A officials. Agencies may also identify disinformation by monitoring trending topics on social media. For example, in 2022, U.S. embassy officials in Prague detected disinformation trending on Czech social media alleging that the U.S. government was planning to move "biolabs" from Ukraine to the Czechia. In response, State's European Bureau released information debunking these false claims.

Agency officials said they rely on additional techniques for social media analysis, such as:

- **Network analysis** involves tracking how various audiences distribute messages on social media, which may provide insight into the strength and impact of different types of messages, according to GEC officials.
- **Natural Language Processing** involves the interpretation of natural human language by machines. Natural Language Processing may be used to automate the process of monitoring and detecting disinformation contained within social or news media.
- **Synthetic Content Detection** is an emerging technique being developed by GEC and private sector partners. According to GEC officials, these techniques analyze images, videos, and text for evidence of synthetic media, which is content that has been artificially produced or modified by an artificial intelligence algorithm. This may include artificially produced video content such as deepfakes, or fake social media profile pictures.[16]

News media analysis. U.S. agencies including State, I&A, and DOD may assess domestic news media, foreign news media, or both as appropriate for evidence of foreign disinformation.[17] For example, U.S. embassy officials overseas monitor local news media and identify suspicious narratives that might be foreign disinformation. Linguistic and regional experts familiar with foreign disinformation actors' strategic interests and common tactics also monitor foreign news media to detect disinformation.

Additionally, foreign disinformation actors may use other countries' media outlets to disguise disinformation and give an appearance of authenticity. For example, the PRC has acquired ownership stakes in foreign media outlets and has sponsored online influencers to legitimize and amplify deceptive messaging, according to State officials. Agency officials said that they track media narratives to assess the degree to which foreign state and non-state actors are manipulating or controlling the content and flow of information.

Monitoring official foreign government sources. GEC and I&A monitor and analyze foreign government communications, such as state-owned media or official government statements, for disinformation campaigns. As noted earlier, some foreign governments, such as Russia and PRC, often spread disinformation via these communications.

Monitoring proxy and cyber-enabled sources. GEC analysts detect disinformation from proxy or cyber-enabled sources by investigating publicly available information and by accessing classified intelligence reporting. GEC officials said that proxy websites connected to foreign governments are not obvious and therefore can lead to disinformation appearing as real information.

Foreign government reporting. GEC and DOD participate in information sharing activities with foreign allies and partners related to disinformation. According to GEC officials, these activities may involve comparing information to validate the existence of suspected disinformation threats, or the sharing of information on new disinformation threats yet unknown to U.S. agencies. For example, GEC coordinates closely with the European Union's Diplomatic Service to share information on emerging threats and share methodologies for data analysis.

Intelligence reporting. State, I&A, and DOD officials told us that they also analyze reporting from U.S. intelligence agencies to identify and monitor foreign disinformation actors. In an upcoming report, we plan to evaluate U.S. agency efforts, including those by the intelligence community, to share information and coordinate their actions to counter foreign disinformation. We plan to issue this report in 2025.

Agency Comments

We provided a draft of this report to DOD, DHS, State, and ODNI for review and comment. DOD, DHS, State, and ODNI provided technical comments, which we incorporated as appropriate.

How GAO Did This Study

Our review focused on fiscal year 2019 to August 2024, and on the Departments of State, Defense, Homeland Security, and ODNI. We identified these agencies through background research and meetings with U.S. agency officials, including those within State, DHS, DOD, and State's Office of Inspector General. In these meetings, we asked officials to identify the relevant components both in their agencies and throughout the federal government that conduct activities to counter foreign disinformation. We also interviewed knowledgeable stakeholders from the RAND Corporation to discuss their work on U.S. adversaries' efforts to spread foreign disinformation.

To describe U.S. agency efforts to define foreign disinformation, we interviewed agency officials and reviewed the National Intelligence Council's *Updated IC Lexicon for Foreign Malign Influence.*[18] To describe U.S. agency efforts to detect foreign disinformation, we interviewed agency officials and reviewed agency documents to understand detection sources and techniques used by these agencies. To describe the legal authorities used by U.S. agencies to counter foreign disinformation, we asked U.S. agency officials to identify relevant authorities and reviewed the legal provisions they identified.

We conducted this performance audit from October 2023 to September 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

List of Addressees

The Honorable Jamie Raskin
Ranking Member
Committee on Oversight and Accountability
House of Representatives

The Honorable Robert Garcia
Ranking Member
Subcommittee on National Security, the Border, and Foreign Affairs
Committee on Oversight and Accountability
House of Representatives

The Honorable John Fetterman
United States Senate

The Honorable Stephen F. Lynch
House of Representatives

We are sending copies of this report to the appropriate congressional Committees; the Secretaries of State, Defense, and Homeland Security, and the Director of National Intelligence; and other interested parties. In addition, the report is also available at no charge on the GAO website at https://www.gao.gov.

GAO Contact Information

For more information, contact: Chelsa Kenney, Director, International Affairs and Trade, KenneyC@gao.gov, (202) 512-2964.

Sarah Kaczmarek, Managing Director, Public Affairs, kaczmareks@gao.gov, (202) 512-4800.

A. Nicole Clowers, Managing Director, Congressional Relations, ClowersA@gao.gov, (202) 512-4400.

Staff Acknowledgments: Jaime Allentuck (Assistant Director), Teresa Abruzzo Heger (Analyst-in-Charge), Karl Antonsson, Tommy Baril, Pamela Davidson, Neil Doherty, Anna Sophia Lindholm, Grace Lui, Donna Morgan, and Alex Welsh.

Endnotes

[1]50 U.S.C. § 3059(b)(4). The FMIC must also provide these assessments, indications and warnings with regard to foreign malign influence campaigns from the Democratic People's Republic of Korea and any other foreign country that the Director of the FMIC determines appropriate.
[2]According to GEC, Russia launders disinformation in Latin America by creating content and sending the material to selected editorial and linguistics staff in Latin America. These staff then review, edit, translate, and ultimately publish the disinformation in local mass media.
[3]As an example of promoting norms for governing digital platforms favorable to PRC's preferences, State/GEC reported that a PRC-state owned company proposed a "smart city" system that could, for example, enhance government control of the region by automatically comparing targets' faces and license plates to blacklists.
[4]The Africa Center for Strategic Studies, *Mapping a Surge of Disinformation in Africa*, March 13, 2024. According to its website, the Africa Center for Strategic Studies is an academic institution within DOD established and funded by Congress for the study of security issues relating to Africa and serving as a forum for bilateral and multilateral research, communication, training, and exchange of ideas involving military and civilian participants.
[5]Statement from Avril Haines, Director of National Intelligence, Senate Select Committee on Intelligence, May 15, 2024.
[6]Among others, we published five related reviews of, respectively (1) DOD's coordination related with foreign partners on cyberspace operations; (2) the technology behind generative artificial intelligence systems and their many uses; (3) the policy and context around combating deepfakes; (4) DOD's use and protection of the information environment through ubiquitous and malign information, threat actors, and threat actions, among other things; and (5) the U.S. government's approach to addressing Russian disinformation overseas. See *Cyberspace Operations: DOD Should Take Steps to Improve Coordination with Foreign Partners*, GAO-24-103716C (Washington, D.C.: July 25, 2024); *Artificial Intelligence: Generative AI Technologies and Their Commercial Applications*, GAO-24-106946 (Washington, D.C.: June 20, 2024); *Science & Tech Spotlight: Combating Deepfakes*, GAO-24-107292 (Washington, D.C.: March 11, 2024); *Information Environment: Opportunities and Threats to DOD's National Security Mission*, GAO-22-104714 (Washington, D.C.: September 21, 2022); *Russia: U.S. Government Takes a Country-Specific Approach to Addressing Disinformation Overseas*, GAO-17-382C (Washington, D.C.: May 2, 2017).

[7]The Department of Justice's Federal Bureau of Investigation (FBI) is the lead federal agency for investigation of foreign influence operations and leads the Foreign Influence Task Force. According to FBI officials, this task force counters foreign malign influence actors, not foreign disinformation.
[8]50 U.S.C. § 3059(b)(1).
[9]National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114–328, Div. A, Title XII, § 1287, 130 Stat. 2000, 2546-8 (Dec. 23, 2016) (FY17 NDAA), as amended by John. S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115–232, Div. A, Title XII, § 1284, 132 Stat. 1636, 2076-8 (Aug. 13, 2018), codified as amended at 22 U.S.C. § 2656 note, Global Engagement Center. State established the State/GEC in 2016 in response to a provision in the FY17 NDAA and Executive Order 13721. *Developing an Integrated Global Engagement Center To Support Government-wide Counterterrorism Communications Activities Directed Abroad and Revoking Executive Order 13584*, 81 Fed. Reg. 14685 (March 15, 2016). State/GEC's statutory authority outlines 11 specific functions. Consistent with its statutory authority, State/GEC proactively promotes credible, fact-based narratives and policies to audiences outside the United States, according to agency officials.
[10]DHS's Cybersecurity and Infrastructure Security Agency, *Tactics of Disinformation.*
[11]The National Intelligence Council defines foreign malign influence as 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.
[12]Additional information regarding DOD activities to counter foreign disinformation is classified.
[13]National Intelligence Council Memorandum 2022-17680, *Updated IC Lexicon for Foreign Malign Influence* (Aug. 19, 2022).
[14]According to the statute that established the FMIC, the term "foreign malign influence" refers to 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 objective of influencing, through overt or covert means 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 the public opinion within the United States. Covered countries identified in FMIC's statues are Russia, China, Iran, and North Korea. 50 U.S.C. § 3059(f)(2). Additional legal authority for the FMIC is derived from 50 U.S.C. § 3058. ODNI considers the Lexicon definitions to align with the authorities found in both 50 U.S.C. § 3058 and 50 U.S.C. § 3059.
[15]DOD Components acquire, assess, and use information that is available to the American public and consumers worldwide to plan, inform, enable, execute, and support a wide range of DOD missions, according to DOD officials. These missions include the department's foreign intelligence and cybersecurity missions, security activities, and protecting DOD personnel and information from foreign adversary threats. According to DOD officials, these activities are conducted responsibly and in accordance with all applicable laws, including the Fourth Amendment to the Constitution, the Foreign Intelligence Surveillance Act of 1978, the Privacy Act of 1974, and DOD's implementing policies.
[16]GAO, *Science and Tech Spotlight: Deepfakes,* GAO-20-379SP (Washington, D.C.: February 20, 2020).
[17]According to DOD officials, DOD only assesses U.S. media to inform Public Affairs releases and statements.
[18]National Intelligence Council Memorandum 2022-17680, *Updated IC Lexicon for Foreign Malign Influence* (Aug. 19, 2022).

Additional source information for images, tables, or figures in this product when that information was not listed adjacent to the image, table, or figure. Page 3: somartin/stock.adobe.com (flag); page 4: somartin/stock.adobe.com (flags); page 5: Semper Fidelis/stock.adobe.com (seal); page 6: Semper Fidelis/stock.adobe.com (seal); page 7: Semper Fidelis/stock.adobe.com (seal); table 2: Semper Fidelis/stock.adobe.com (seals).