

The Trump Administration's Withdrawal from the Fight Against Foreign Interference—Strategic Implications

David Siman-Tov | No. 2006 | July 7, 2025

Donald Trump's return to the White House in January 2025 signaled dramatic changes in how the United States addresses threats of foreign influence and interference in the digital realm. The administration swiftly moved to dismantle government mechanisms that had been established in previous years to protect the United States from hostile foreign influence. These steps—from the dismissal of senior security officials to the shutdown of dedicated teams in government departments—raise concerns about the West's overall capacity to confront foreign interference campaigns by Russia, China, and Iran. The absence of protective efforts lays fertile ground for an increasing spread of foreign influence campaigns, which could even alter the global balance of power. This article analyzes the key rollback measures taken by the Trump administration in the context of the struggle against foreign interference and surveys their direct and indirect consequences for the fight against disinformation in the West and in Israel.

Foreign Interference and the US Counter-Strategy After 2016

Following revelations of Russian interference in the 2016 presidential election, Washington adopted a structured national policy to confront the threat of malicious foreign influence. Intelligence leaders and members of Congress defined a strategy aimed at “protecting democratic institutions and public trust; developing a shared operational picture; and reducing adversaries’ asymmetric advantages.” The core objective was to “protect democratic processes and public trust by identifying, preventing, and deterring malign influence operations by foreign adversaries, without infringing on constitutional freedoms.” This strategy relied on interagency cooperation, led and coordinated by the National Security Council. It included the establishment of dedicated bodies within the intelligence community, the State Department, and the Department of Homeland Security, as well as legislative measures to support the policy. Its effectiveness was evident during the 2020 elections cycle, which were described as “the most secure in history.” An [intelligence report](#) published a year later concluded that attempts to influence the elections through cognitive interference had been detected and thwarted.

Dismantling of US Disinformation-Fighting Mechanisms

On January 20, 2025, during the signing ceremony for Executive Order 14149, President Trump declared the end of censorship of free speech: “Government censorship of speech is intolerable in a free society.” This statement reflected an ideological worldview that had

gained traction within the American right over the past decade, based on the premise that federal government entities lack the authority to determine what content is true or false. Critics argued that government agencies had previously removed online content published by conservative actors, claiming it was disinformation. Consequently, all federal activity involving the monitoring, flagging, or removing of content would be perceived as political overreach and as a violation of civil liberties—and therefore must stop.

Although this move was intended to curtail domestic restrictions on freedom of speech in the United States, it has dramatic implications for addressing Foreign Information Manipulation and Interference (FIMI)—a threat widely recognized in the West.

In the early months of Trump's new term, the administration undertook broad steps to dismantle or weaken federal bodies designed to monitor and counter foreign interference in the digital information domain. These included:

- **Shutdown of the FBI's Foreign Influence Task Force:** In February 2025, Attorney General Pam Bondi ordered the dissolution of the Foreign Influence Task Force—the team dedicated to investigating foreign influence and disinformation campaigns, including election interference. The Department of Justice justified the move by stating it aimed “to free resources to address more pressing priorities, and end risks of further weaponization and abuses of prosecutorial discretion.” Former FBI officials criticized the decision, comparing it to “taking a cop off the street during a crime wave.”
- **Suspension of Election Protection Activities at the Department of Homeland Security:** Simultaneously, the White House reduced operations of the expert team at the Cybersecurity and Infrastructure Security Agency (CISA), which had worked to **counter disinformation** and protect election systems. Team members were placed on forced leave and prohibited from continuing their work—even though [intelligence agencies](#) had reported extensive foreign [interference attempts](#) during the 2024 elections.
- **Closure of the Center for Countering Foreign Information Manipulation and Interference at the State Department:** In April 2025, the State Department adopted a “zero-content-involvement” policy. The process had already begun in December 2024, when the budget mandate for the Global Engagement Center (GEC) expired; since then, the center had operated in a limited capacity. Notably, the GEC was founded in 2016 to coordinate and execute strategic communications efforts against Russian foreign influence. On April 16, Secretary of State Marco Rubio [announced](#) its official dismantling. In a statement on the Department's website, he claimed the office spent more than \$50 million annually, censoring Americans' voices and declared that “the American people don't need a shadow agency to protect them from lies.”
- **Dismissal of the NSA Chief:** In early April 2025, President Trump unexpectedly fired General Tim Haugh, who headed the National Security Agency (NSA) and also commanded the Pentagon's US Cyber Command. Haugh—a 33-year intelligence and

cyber operations veteran—and his deputy were dismissed for what was described as “[disloyalty to the president](#).” Some [view the dismissal](#) as part of a broader policy trend undermining deterrence and capabilities meant to prevent foreign interference, given the NSA’s key role in combating Russian troll farms.

- **Weakened Enforcement of Laws Against Foreign Influence:** Beyond dismantling institutions, the Trump administration scaled back legal tools used to fight foreign influence. The new Department of Justice leadership effectively froze enforcement of the Foreign Agents Registration Act (FARA)—a law previously used to prosecute American citizens secretly funded by foreign governments for political activity. In addition, the program initiated under the Biden administration to target the assets of Russian oligarchs, implemented as part of the sanctions against Russia, was canceled in early 2025—a move that drew criticism for diminishing US leverage over the Kremlin.
- **Impact on Meta:** In addition to government-level actions, President Trump’s new policy also affected Meta, which [announced](#) in early March 2025 that it was suspending its fact-checking project for political content in the United States until further notice. A company spokesperson explained that the decision aligned with the regulatory environment shaped by President Trump’s directives.

The Growing Role of Civil Society

The federal retreat from the institutional fight against disinformation has highlighted the growing role of civil society in confronting hostile disinformation efforts. For example: [Common Cause](#), a civic organization, expanded its program involving thousands of volunteers who operate a national reporting hotline, monitor voter inquiries in real-time, and cross-reference them with OSINT systems to detect bots and suspicious accounts. The organization’s website describes this as a “critical line of defense against suppression of voting and misleading information ” and notes an increase in volunteer participation, especially during election periods.

Another initiative is the [Election Integrity Partnership](#) (EIP), established to provide rapid response to election-related disinformation in the United States. This coalition includes leading academic institutions and tech organizations. Its activities include real-time identification of false rumors and narratives about voting, analysis of the infrastructure through which disinformation spreads, distribution of corrections and reliable counter-messages, and systematic documentation of disinformation actors and their methods.

At the same time, civil society has become an alternative to government in reporting inauthentic behavior to digital media platforms. One example is the [Alliance for Securing Democracy](#), a US–German initiative aimed at developing comprehensive strategies to deter authoritarian regimes from undermining democracies. The alliance’s website offers an open API to enable decentralized detection as a substitute for government alerts. Suspect data is shared—through cooperation with NATO’s official [STRATCOM](#) center—with digital platforms for removal.

The European Union's Response

In Europe, the Trump administration's withdrawal from federal monitoring frameworks has been interpreted as a wake-up call, exposing a systemic gap in the West's ability to detect and respond to strategic information warfare. For instance, EU DisinfoLab, a Brussels-based watchdog, issued an urgent appeal for the European Union to fill the void and prevent coordinated influence attacks. There were additional calls to establish strategic coordination centers to develop AI-based tools for detecting manipulative content during election periods.

During the NATO foreign ministers' meeting held in Antalya on May 15, Secretary-General Mark Rutte [announced](#) that the US policy change would necessitate expanding NATO's influence operations research center in Riga. Simultaneously, Germany, France, and the Czech Republic launched the [European Democracy Shield](#)—an intelligence-content network that integrates algorithmic models to detect propaganda and provide early warnings to member states. The [European Parliament proposed](#) expanding the Rapid Alert System, an intergovernmental EU coordination mechanism for sharing disinformation alerts, to also ingest OSINT data from American civil society organizations—thereby closing the intelligence gap left by the closure of the US State Department's GEC.

This series of developments carries strategic significance on two levels: Domestically, the European Union assumes the role of “gatekeeper,” strengthening enforcement of its Digital Services Act (DSA) regulations—targeting both platforms and foreign media entities. Internationally, the European Union demonstrates its ability to organize without US leadership, signaling to adversaries that the democratic front is not defenseless.

Conclusions and Implications for Israel

The Trump administration's policy shift—reducing government activity to defend against foreign interference and disinformation, and adjusting expectations from platforms regarding their role—has profound implications for both domestic discourse in the United States and opportunities for influence by hostile foreign states and organizations. Although the new approach is framed in the language of free speech, it exposes the United States' vulnerabilities to digital attacks from Russia, China, and Iran, and weakens deterrence that had begun to take shape in recent years. This shift has dramatic consequences—still too early to fully assess—for the West's ability to counter foreign influence as a strategic threat, especially due to platform policies that align with the current US administration, given the global leadership role traditionally held by the United States.

To fill the gap, civil society actors are stepping in, but lack the authority, intelligence capabilities, and resources for a full-scale response, making their efforts partial and fragmented. In parallel, EU actors are expanding efforts to expose strategic influence operations against the West. Moreover, the European Union, now focused squarely on the FIMI threat, is attempting to enforce compliance by compelling digital platforms to comply with European standards rather than American ones—especially regarding transparency and the removal of inauthentic and malicious content.

Israel, which has been subjected in recent years—and with particular intensity since October 7, 2023—to influence campaigns, cannot afford to remain passive and must act with urgency and determination to address these threats.

Key Policy Recommendations

1. Between the US and EU models, the European Union’s approach offers considerable advantages. The European Union has recognized foreign influence (FIMI) as a central threat and has integrated advanced AI capabilities to detect malicious operations—without infringing on free speech.
2. While freedom of expression is also a protected fundamental right in the European Union, policymakers there understand that external threats endanger the genuine exercise of that freedom. The European Union’s conceptualization of the threat and its policy toolkit offer Israel a model for developing national frameworks and capabilities to mitigate rising risks.
3. Civil society offers a critical advantage in confronting foreign influence and interference, given that such efforts often resonate within domestic discourse. Therefore, Israel should strengthen emerging capabilities, deepen coordination and cooperation, and forge partnerships with relevant actors in Western democracies.

Editors of the series: Anat Kurtz, Eldad Shavit and Ela Greenberg