Copyright 2026 Treadstone 71. Reproduction without written permission is prohibited.

Foreign AI and the Midterm Vote

Plain edition of Public Attribution Series dossier 1. What US bodies said, what vendors found, and what stays unnamed. Treadstone 71, 12 October 2026.

DATE	19 October 2026
AUTHOR	Treadstone 71
STATUS	Final
EDITION	Plain executive edition. Companion to the academic version of the same title.

Twenty-two days before the vote, no US executive agency has said on the record that AI-enabled foreign influence targets the midterms. No vendor report ties such an operation to them either. Researchers do describe a Russian network that pushes doctored video onto American screens, and one account adds altered audio. The Washington Post reported on 4 October that a National Intelligence Council product, still held back, ranks Russia first and marks rising AI use. Anonymous sources carry it. Read the quiet as a hole in the record. Safety is a separate claim.

TL;DR

A client who reads only US sources sees quiet and calls it calm. The record breaks that reading. Meta removed an Iran-origin network that posed as US activists and pushed AI-made posts about American politics. The company tied it to no named Iranian body and to no election. Press accounts describe Matryoshka videos built from real faces and bent speech, dressed in the logos of CNN, the BBC and the New York Times. Four calls stand. A 12 October refresh moved none of them.

BLUF

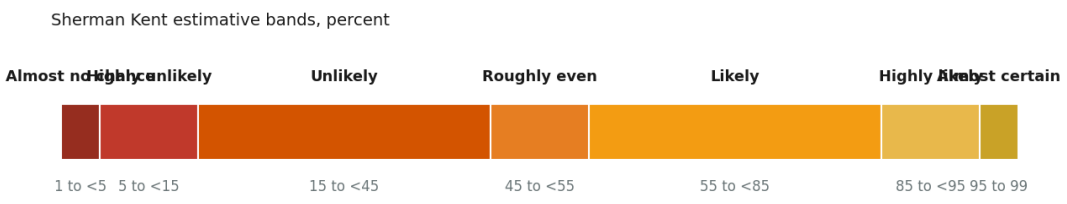


Figure 1. Sherman Kent estimative bands. Every judgment in this edition carries one of these likelihood terms.

Who. Iran works through three bodies here: the Islamic Culture and Communications Organization, the Islamic Propaganda Office of Khorasan Razavi, and the Bina Cultural Observatory, beside the IRGC channels @hamyane_sepah and @moghavematnews_iran. Russia runs Matryoshka, which others call Operation Overload and Microsoft tracks as Storm-1679, and CopyCop, tracked as Storm-1516. China fields Spamouflage, with no midterm item on file. The US side holds the White House, the Departments of War, Justice, State and Homeland Security, the FBI, ODNI, CISA, NSA, the Election Assistance Commission, NASS, NASED and the Congress.

What. The executive record holds four texts on foreign danger to the vote. None names AI. No adversary gets named either. Vendors have reported AI-enabled influence that reached American audiences, and none of it ties to the midterms. Only the Congress holds a paper that puts Russia, AI and the vote in one letter, and members of Congress are no executive agency.

So what. A reader who treats silence as safety gets it wrong. The same record shows the Iranian network Meta pulled and press accounts of Russian fakes aimed at American eyes. Brand misuse is the reach that touches every firm. Matryoshka wraps its fakes in real news logos. A company with a logo faces that same treatment. The brand link is our read, and the sources stop short of stating it.

Why now. The vote falls on 3 November. A War Department directive on election defense carries a memo of 22 September and a release of 28 September. Press accounts date the Matryoshka wave from about 10 September. OpenAI published two false-front cases on 8 October. Senators Padilla and Schiff asked seven company heads to reply by 15 October. Representative Himes and Senator Warner want a classified update from the Director of National Intelligence by 31 October. The window for a federal statement shuts on election day.

Impacts so far. No source measures a shift in belief or behavior. Reach is the whole of what gets counted. Meta says 79,400 accounts followed the Iran-origin network. Mother Jones counts about 155,000 views in a day for one fake and nearly 200,000 for another, then reports that bots pumped both and the real audience ran to a few thousand. The ISD found limited spread for the same network in Germany. NewsGuard logged 23 viral false claims about the midterms across 328 appearances on 9 October and tied none to a foreign actor. No outcome in the record changed because of AI.

Outlook. Two events frame the next 22 days. A US federal agency naming the threat on the record sits at 26 percent, Unlikely (15 to <45), Low confidence. Documentation by a platform, vendor or state election official sits at 40 percent, Unlikely (15 to <45), Low confidence. The platform case beats the agency case, because platforms publish on their own clock while agencies hold back. Stretched to 9 November, the likely path runs through hoax threats and fake graphics on 3 and 4 November, a House statement on 4 November, and a federal line of no material effect by 9 November at 71 percent, Likely (55 to <85), Low confidence.

The quiet in the US record

Four executive texts speak to foreign danger around the vote. Not one names AI. None points at a country. The War Department directive orders Cyber Command and three agencies to work

election threats, and it leaves AI unmentioned. Seven executive bodies, Justice and State and the White House among them, carry no item from 1 September forward on AI-enabled influence targeting the midterm vote.

Agencies publish on their own terms, and a missing line proves neither danger nor safety.

A hole is not a verdict.

What vendors and platforms found

Platforms and labs carry the firmer facts. Meta pulled a network of Iranian origin that impersonated US activists and ran machine-made posts on American politics. The company named no Iranian body behind it and tied it to no election. On 8 October, OpenAI set out two more false fronts. NewsGuard watches viral election claims and attributes none abroad.

One habit runs through these reports. The verified fact and the adversary claim stay in separate sentences. A face in a video is a fact. The voice laid over it is the claim.

The dossier keeps the two apart.

The one named operation: Matryoshka

Matryoshka is the single foreign operation the record names against American audiences, and the naming comes from researchers rather than from an agency. The network copies real newsrooms. It stamps the marks of the BBC, CNN and the Times onto fabricated clips. Graphika's own page on the wave points to Operation Overload as the source and says nothing about AI.

So the brand theft is documented. The AI label on the clips is press description, not vendor finding.

What stays unnamed

Much of the picture has no owner. No agency has released the National Intelligence Council product that ranks Russia first. Whether any clip changed a single vote stays unmeasured. The biggest view counts belong to networks that no source ties to AI output.

Attribution thins as a claim climbs toward a headline, and the dossier marks each step.

The four calls

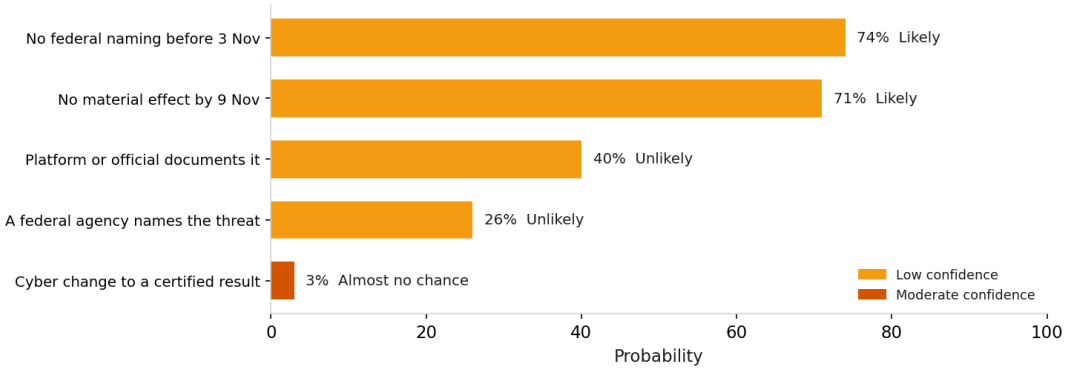


Figure 2. The quantified calls, by probability and shaded by confidence. A cyber change to a certified result sits at Almost no chance.

Four judgments carry the dossier, and each one holds at Low confidence. First, no federal agency will name AI-enabled foreign influence aimed at the midterms before 3 November, at 74 percent, Likely (55 to <85). Second, the best-evidenced foreign AI aimed at American political audiences stays that Iranian network. Third, documentation by a platform or state official is likelier than any agency statement. Fourth, through 9 November adversaries will work the perception of the count rather than the count, and a cyber change to any certified result sits at Almost no chance (1 to <5), Moderate confidence.

A refresh on 12 October put every call against the newest facts.

No number moved.

Watch items to 3 November

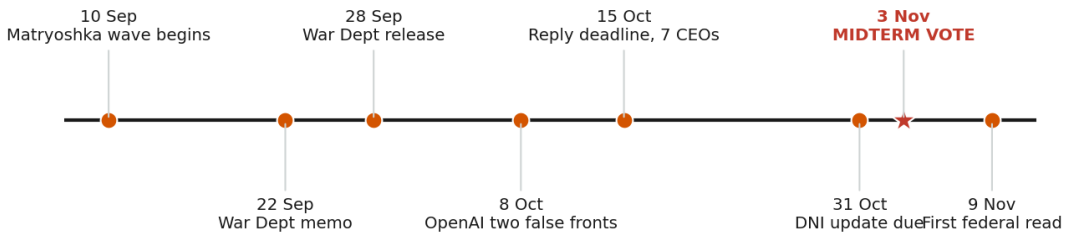


Figure 3. The why-now clock, 10 September to 9 November. The vote on 3 November is the fixed point, with the first federal read on effect five days later.

A short set of dates carries the risk. The reply deadline for seven company heads lands on 15 October. A classified update to the intelligence chief is due by 31 October. Hoax bomb threats and fake result graphics tend to cluster on the vote itself and the morning after. Watch 3 and 4 November for staged screenshots, and watch 9 November for the first federal read on effect.

How to read this

Quiet in American sources is a logged search result that carries no verdict.

The firm exposure that reaches readers of this edition is brand misuse, since any logo can ride on a fake.

Guard the logo. Check the video. Trust the count, which stays the hardest target on the board.