Russia, Iran, and China continue influence campaigns in final weeks before Election Day 2024

A MICROSOFT THREAT INTELLIGENCE REPORT

Date: October 23, 2024

This fifth Microsoft Threat Analysis Center (MTAC) report of the 2024 presidential election cycle provides a final assessment of Russia, Iran, and China's influence operations heading into the final two weeks before Election Day.

Since our last two reports, the U.S. government has taken many actions revealing cyber and influence activity from foreign adversaries related to election 2024. On September 18, the Office of the Director of National Intelligence (ODNI), FBI, and CISA published a joint statement revealing Iranian malicious cyber actors' sending of "stolen, non-public material from former President Trump's campaign" to both individuals then associated with President Biden's campaign and U.S. media organizations.[1] On September 27, the Department of Justice (DOJ) indicted three Islamic Revolutionary Guard Corps (IRGC) cyber actors for the Iranian hack-and-leak operation targeting the Trump-Vance campaign. This cyber-influence activity was, as the DOJ notes, part of Iran's "continuing efforts to stoke discord, erode confidence in the U.S. electoral process, and unlawfully acquire information relating to current and former U.S. officials that could be used to advance the malign activities of the IRGC, including ongoing efforts to avenge the death of Qasem Soleimani, the former commander of the IRGC – Qods Force."[2]

Our last report also noted that while Iranian actors have focused their cyber-influence operations on the Trump campaign, Russian influence actors decisively pivoted toward the Harris campaign once she entered the race. In the month since our fourth election report on September 17, 2024, we have observed Russian actors integrating generative AI into their U.S. election influence efforts, including the creation of a political deepfake of Vice President Harris that garnered little online engagement.

Iranian groups tasked with targeting the U.S. elections may make an effort—as they have in the past—to run influence operations both shortly before and soon after the election by leveraging cyber intrusions from weeks to months prior. Last week, on October 14, an online persona operated by Iran began falsely posing as an American and called on Americans to boycott the elections due to both candidates' support for Israel's military operations. This recent activity, along with Microsoft findings from earlier this year, suggest Iran is gearing up for additional influence operations close to Election Day.

Chinese influence operations have recently taken a new turn shifting focus to several down-ballot candidates and members of Congress. In one case, Chinese influence actor Taizi Flood

[1] https://www.fbi.gov/news/press-releases/joint-odni-fbi-and-cisa-statement-091824

[2] https://www.justice.gov/opa/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us

conducted a small-scale campaign denigrating a Republican candidate up for re-election while promoting the candidate's Democratic opponent.

Our final report concludes with some scenarios to look for in the final days before the election and on Election Day.

Additional signs of Iranian preparation for influence operations arise

On October 14, an Iranian operated cyber persona called on Americans to boycott U.S. elections and sought to stoke university protests. The group, "Bushnell's Men," which poses as Americans on social media, used Telegram and X (formerly Twitter) to call on Americans to sit out the elections, sending the message that the next U.S. president won't have their support for "aiding Israel in its brutal activities." Bushnell's Men previously sought to stoke anti-Israeli university protests in the United States and Europe in May, in part by remotely printing fliers calling for demonstrations. The group's latest messaging continues to stoke anti-Israeli protests at universities, linking the election boycott to a lack of a ceasefire and claiming that the "Pro-Palestine Student Movement is Still alive" [sic].

Since our last elections report in September 2024, Microsoft discovered that Cotton Sandstorm (a.k.a. Emennet Pasargad) performed reconnaissance and limited probing of election-related websites in some U.S. swing states in April 2024. Cotton Sandstorm, which is directed by the IRGC, also conducted reconnaissance of major U.S. media outlets in May 2024.

Cotton Sandstorm's springtime cyber operations may represent preparations for the 2024 election. Historically, Cotton Sandstorm has targeted elections in a similar fashion through hacking operations aimed at media entities and state election-related websites ahead of the last U.S. presidential election.[3] In 2020, Cotton Sandstorm launched its first cyber-enabled influence operation just two weeks ahead of the elections, running an email campaign posing as the right-wing "Proud Boys," threatening Florida residents to "vote for Trump or else!"[4] Following the election, Cotton Sandstorm ran a separate operation, which called for violence against U.S. election officials who claimed the elections were secure or denied claims of widespread election fraud.[5]

We have not yet observed Cotton Sandstorm launching influence operations targeting these elections, but MTAC expects Cotton Sandstorm will increase its activity as the election nears given the group's operational tempo and history of election interference. In the last year, Cotton Sandstorm developed a regular pattern of running multiple, simultaneous operations roughly every three to ten weeks. Microsoft detected Cotton Sandstorm running its last

[3] home.treasury.gov/news/press-releases/jy0494

[4] s3.documentcloud.org/documents/25176482/us_v_seyyed_mohammad_hosein_et_al_signed_indictment_redacted-1.pdf

[5] fbi.gov/news/press-releases/iranian-cyber-actors-responsible-for-website-threatening-us-election-officials; nbcnews.com/tech/security/irans-history-elaborate-election-interference-efforts-trump-campaign-h-rcna171312

operation targeting Israel's participation in the Paris Olympics in late July 2024. Therefore, we expect this group may launch another series of influence operations imminently.

Microsoft also observed the IRGC's Mint Sandstorm (a.k.a. APT-42) compromising an account of a notable Republican politician, who had a different account targeted in June, as we previously reported. Microsoft informed the individual in both cases to mitigate the threat.

Another Iran-run group, Storm-2035, has persistently pursued U.S. audiences since we revealed the group's activity in early August 2024. The network's websites posing as local U.S. news outlets has been posting divisive and at times conspiratorial content targeting Democrats and Republicans at a cadence of around eight articles per week per outlet.

On October 18, the FBI and CISA released a warning to American voters about foreign malign influence activity and the spread of disinformation in the final days ahead of the 2024 presidential election.[6] Iranian activity featured in the release, including cyber-enabled influence operations and the inauthentic news sites discussed by our August 9 elections report.[7]

Russian actors' pivot to Harris-Walz campaign features political deepfake

In mid-September, Russian-language accounts on X and Telegram posted an AI-enhanced video of Vice President Kamala Harris. The video falsely depicts her making a crass reference to assassination attempts against former President Donald Trump. In the video, AI-generated audio of Harris states that Trump refused to "even die with dignity."[8] MTAC assesses that Russian influence actors created the deepfake to stoke anger at Harris. The video received tens of thousands of views on X after an RT correspondent posted it on September 23, 2024.[9]

[6] cisa.gov/sites/default/files/2024-10/PSA_Just%20So%20You%20Know_Foreign_Threat_Actors_Likely_to_Use_a_Variety_of_Tactics.pdf

[7] cisa.gov/sites/default/files/202410/PSA_Just%20So%20You%20Know_Foreign_Threat_Actors_Likely_to_Use_a_Variety_of_Tactics.pdf

[8] x.com/hd7PR5YZbN59013/status/1836354369672937642

[9] x.com/BowesChay/status/1838223592703524902

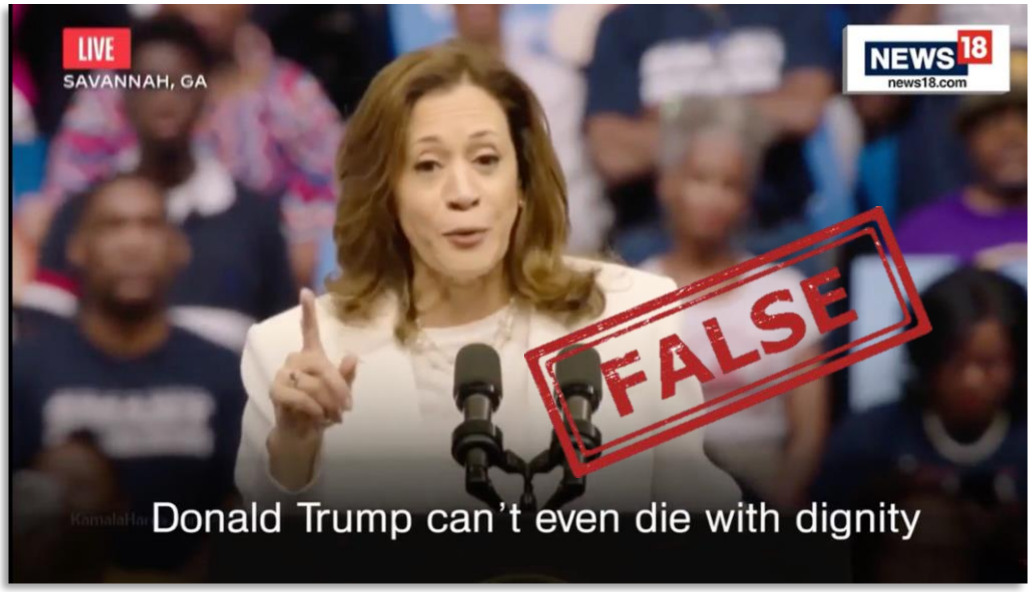


Figure 1: A still from the deepfake of Vice President Kamala Harris created by Russian influence actors. The AI-enhanced video falsely portrayed Harris as saying former President Trump could not "even die with dignity."

The ODNI confirmed in September 2024 that the U.S. intelligence community observes Russia using both AI-generated content as well as traditional techniques in influence operations.[10] While Russian actors have used AI at times, most Kremlin-backed campaigns continue to employ simple tactics—such as deceptive editing, spoofs, and staged videos—in their targeting of Vice President Harris.

ODNI's reporting confirmed our own September 17 findings that Russian influence actor Storm-1516 staged a video framing Vice President Harris in an alleged hit-and-run incident. The Storm-1516 video received millions of impressions across social media illustrating how, to date, traditional and more rudimentary influence techniques have much more impact and reach than AI-enhanced or AI-generated content.

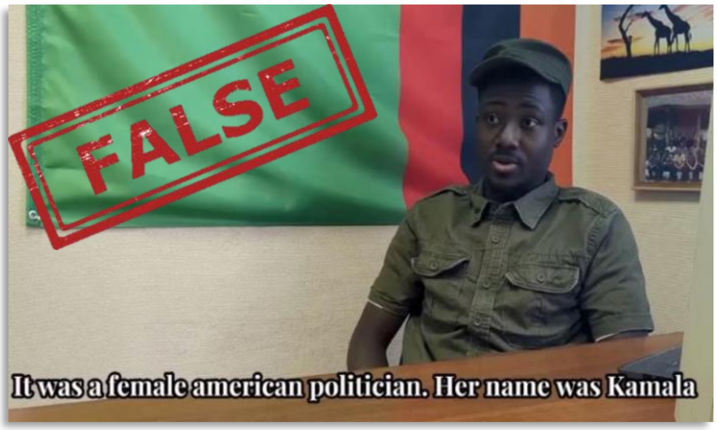


Figure 2: A still from the Storm-1516 video accusing Harris of illegal poaching in Zambia. The video used the historical tactics of Storm-1516, including an on-camera interview and amplification patterns.

On September 25, 2024, a Storm-1516 video depicted a staged interview with a park ranger impersonator who claimed Harris killed an endangered rhinoceros in

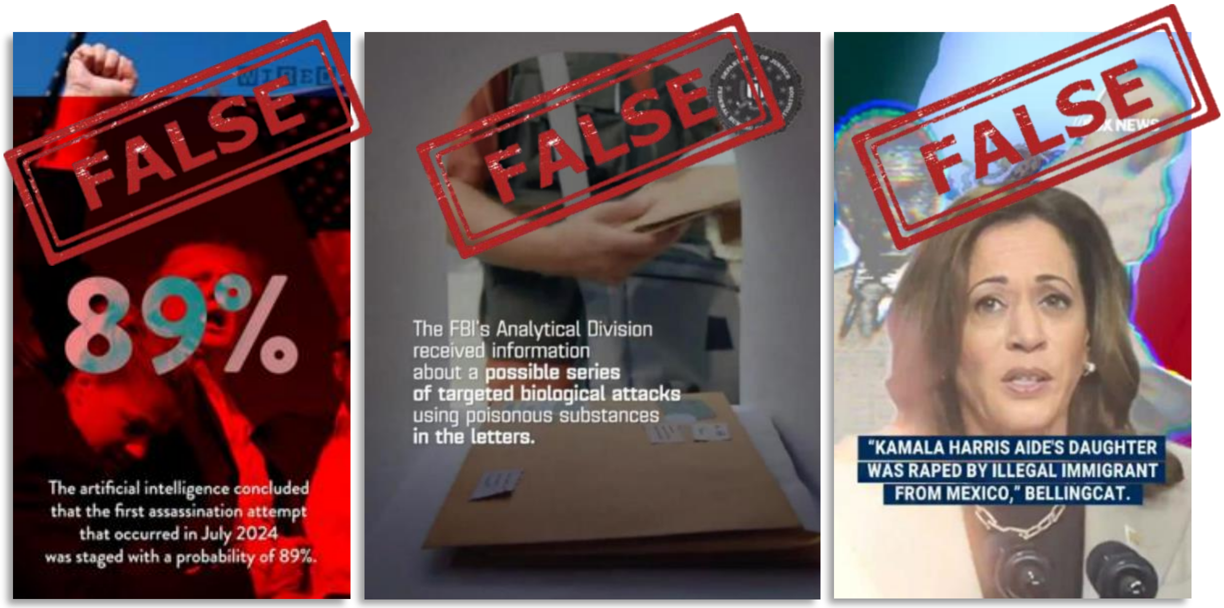
[10] odni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240923.pdf

Zambia. The story was amplified through Storm-1516-affiliated websites and channels. Like most of Storm-1516's content, the video is clearly scripted and unconvincing. However, Storm-1516's strengths lie in fabricating superficial backlogs of evidence supporting sensational narratives rather than creating high-quality content capable of withstanding thorough scrutiny. This video appeared on a YouTube channel purpose-built for this video's upload; the channel, as of this writing, has not uploaded any other videos. Later, a correspondent for state-sponsored media outlet RT amplified the video's narrative on social media, linking to a website previously involved in Storm-1516 operations which repeats the story and links to the YouTube video. The coordination between Storm-1516 content production and amplification from personnel openly affiliated with RT and Sputnik has at times created a much larger reach for Russian disinformation into English-language audiences.

On October 16, a video emerged on X depicting an individual accusing Governor Tim Walz of sexual assault while a student at Mankato West High School.[11] MTAC assesses with moderate confidence that Storm-1516 is responsible for this video, which shows signs of manipulation. As the video gained engagement, online fact-checkers identified the video as manipulated; however, other researchers remain uncertain about both the potential type and degree of manipulation. The initial video garnered nearly 5 million views on X in fewer than 24 hours and many additional copies of this video were detected on several social media platforms.

The Russian influence actor tracked by Microsoft as Storm-1679 produced additional fake election-related content using its routine tactic of spoofing reputable media outlets. Since the summer 2023, Storm-1679 has routinely uploaded its videos to Russian-language Telegram channels. This process changed in September 2024 when Storm-1679 shifted their content distribution to X and their targeting toward the U.S. election and Vice President Harris. Storm-1679 videos posted to X received higher levels of engagement than those posted to Telegram, demonstrating the actor's ability to reach U.S. audiences on Western platforms. Recent Storm-1679 videos targeting Harris spoof a range of news outlets and organizations, including Fox News, the FBI, and the technology publication Wired.

[11] FACT CHECK: Did A Former Student Accuse Tim Walz Of Sexual Assault?



The artificial intelligence concluded that the first assassination attempt that occurred in July 2024 was staged with a probability of 89%.

The FBI's Analytical Division received information about a possible series of targeted biological attacks using poisonous substances in the letters.

"KAMALA HARRIS AIDE'S DAUGHTER WAS RAPED BY ILLEGAL IMMIGRANT FROM MEXICO," BELLINGCAT.

Figure 3: Stills from Storm-1679 videos focused on the US election spoofing (from left to right) Wired, the FBI, and Fox News.

Finally, the US government published several revelations regarding foreign malign influence activity since our last report. This includes a Rewards for Justice release on several individuals behind Rybar, a media enterprise Microsoft tracks as Volga Flood.[12] In their release, the US State Department references Volga Flood's "TEXASvsUSA" accounts, which MTAC initially reported on in our August 9 elections report.[13] Russian influence operations—primarily activity conducted by the Russian Presidential Administration-backed actor MTAC tracks as Ruza Flood—also appeared in CISA and FBI's October 18 public service announcement.[14]

Chinese online influence campaigns criticize down-ballot Republican candidates

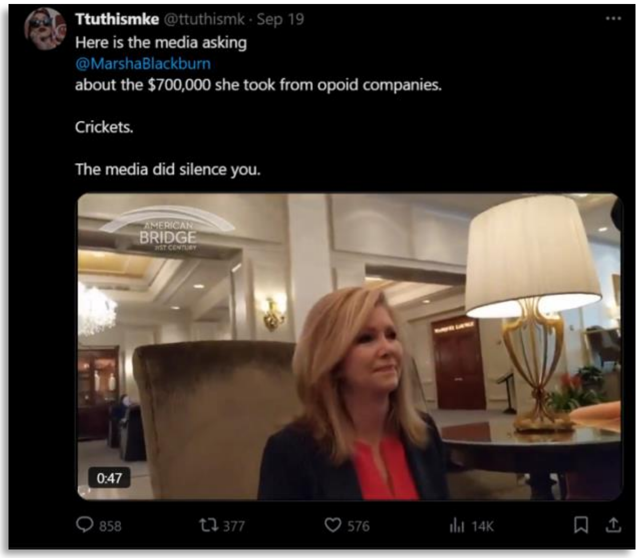
Starting in July 2024 and accelerating in September 2024, the Chinese Ministry of Public Security-linked influence actor Microsoft tracks as Taizi Flood (a.k.a. "Spamouflage") launched campaigns critical of several Republican politicians including candidates up for election this November. The candidates for seats in both the House and the Senate have all publicly denounced the People's Republic of China (PRC), making them attractive targets of Chinese influence operations.

[12] rewardsforjustice.net/rewards/rybar/

[13] cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf

[14] cisa.gov/sites/default/files/2024-10/PSA_Just%20So%20You%20Know_Foreign_Threat_Actors_Likely_to_Use_a_Variety_of_Tactics.pdf

At least one Taizi Flood asset targeted Representative Barry Moore, running for election in Alabama's Second Congressional District, in content criticizing Moore's support of Israel. The Taizi Flood posts about Moore frequently used antisemitic language. The posts received engagement from legitimate online users and were further amplified by other Taizi Flood assets online. At the same time, roughly two dozen Taizi Flood accounts posted various narratives accusing Senator Marco Rubio of corruption and connecting Rubio to criticisms made about the Harris-Walz campaign. MTAC has observed Chinese influence operations targeting Senator Rubio intermittently since the lead up to the 2022 midterm elections.



Ttuthismke @ttuthismk · Sep 19

Here is the media asking
@MarshaBlackburn
about the $700,000 she took from opoid companies.

Crickets.

The media did silence you.

Figure 4: Taizi Flood post about Sen. Marsha Blackburn.

In late September 2024, Taizi Flood launched a campaign criticizing incumbent Tennessee Senator Marsha Blackburn, who is up for reelection in November. Blackburn, a longtime critic of the PRC, is likely an attractive target for Chinese online influence due to these public stances. By early October, Taizi Flood accounts evolved this campaign, promoting Blackburn's opponent in the 2024 election, Representative Gloria Johnson. Although Taizi Flood assets engaged in attention-seeking behavior by tagging prominent politicians, celebrities, and news outlets in relevant posts, the campaign received virtually no authentic engagement as of the time of this writing.

Lastly, beginning in mid-October 2024, a handful of Taizi Flood accounts began accusing Representative Michael McCaul of Texas's Tenth Congressional District of "abusing power for personal gain." Taizi Flood assets on other websites focused on his position as chair of the House Foreign Affairs Committee and "China Task Force," further accusing him of insider trading and pushing for controversial bills.[15] McCaul was previously sanctioned by China in April 2023 following his delegation visit to Taiwan.

Final takeaways

Several foreign malign influence scenarios may emerge in the final two weeks before Election Day. First, we may see increased influence activity, particularly from Iranian actor Cotton Sandstorm, which has a history of election interference. Russian hacktivist groups often overstate their claims or impact of cyberattacks; however, as observed during the 2022

[15] archive.is/pldGX

midterm elections, even simple cyberattacks or claims of them from these cyber proxies can disrupt elections, drive headlines, and undermine trust in the outcome of the vote.[16]

Second, influence actors from all three authoritarian regimes—Russia, Iran, and China—may seek to sow doubt about the integrity of the election's outcome. As MTAC observed during the 2020 presidential cycle, foreign adversaries will amplify claims of election rigging, voter fraud, or other election integrity issues to sow chaos among the U.S. electorate and undermine international confidence in U.S. political stability.

Finally, we expect AI usage to continue through the end of the election cycle, but this AI usage will be a small subset of a much wider swath of digital manipulations thrust onto audiences in the final days of the election. During times of crisis, conflict, and competition, manipulated images, audio, and video often travel further and faster across audiences than during an average news cycle. Russian influence actors, such as Ruza Flood, Storm-1516, and Storm-1679, amplified by Russian state media outlets RT and Sputnik News, have proven nimble and capable of inserting deceptive content and distributing it rapidly at key moments of audience confusion. Early detection and fact checking will be essential for preventing Russia from undermining the fair conduct of the election.

[16] usatoday.com/story/news/politics/elections/2022/11/08/2022-midterm-websites-mississippi-hit-cyber-attack/8308615001