Research memo

America Resilient in the Face of Aggressive Foreign Malign Influence Targeting the 2024 U.S. Elections

By Max Lesser, Mason Krusch, and Ari Ben Am

December 18, 2024

Introduction

America's adversaries did not significantly affect the results of the 2024 U.S. elections — but not for lack of trying. Russia, Iran, and China waged aggressive influence operations targeting America's political system, but America proved remarkably resilient. Efforts of federal and state governments, the private sector, and the research community appear to have thwarted Russian, Iranian, and Chinese efforts to shape voters' preferences and undermine Americans' faith in the fairness and integrity of the democratic process.

Russia aimed to weaken Vice President Kamala Harris's campaign, while Iran sought to undermine President-elect Donald Trump's campaign.[1] Although China targeted several down-ballot candidates it viewed as particularly hostile, Beijing attacked both major presidential candidates. Russia, Iran, and China all also sought to undermine Americans' faith in the democratic process itself.

Hackers also attempted to directly disrupt the voting process. Georgia's secretary of state claimed that an unspecified nation-state actor likely conducted cyberattacks against a website voters use to request absentee ballots.[2] And on Election Day, people using Russian email addresses sent hoax bomb threats to polling stations across multiple

1. Max Lesser, "Foreign Malign Election Meddling Persists But Struggles to Gain Traction," *Foundation for Defense of Democracies*, October 29, 2024. (https://www.fdd.org/wp-content/uploads/2024/10/fdd-memo-foreign-malign-election-meddling-persists-but-struggles-to-gain-traction.pdf); Insikt Group, "Operation Overload Impersonates Media to Influence 2024 U.S. Election," *Recorded Future*, October 23, 2024. (https://go.recordedfuture.com/hubfs/reports/ta-ru-2024-1023.pdf); "Russia, Iran, and China Continue Influence Campaigns in Final Weeks Before Election Day 2024," *Microsoft Threat Analysis Center*, October 23, 2024. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-5-on-Russian-Influence.pdf); "The #Americans: Chinese State-Linked Influence Operation Spamouflage Masquerades as U.S. Voters to Push Divisive Online Narratives Ahead of 2024 Election," *Graphika*, September 2024. (https://public-assets.graphika.com/reports/graphika-report-the-americans.pdf)

2. U.S. Federal Bureau of Investigation, National Press Office, Press Release, "FBI Statement on Bomb Threats to Polling Locations," November 5, 2024. (https://www.fbi.gov/news/press-releases/fbi-statement-on-bomb-threats-to-polling-locations); Gabe Colon, Sean Lyngaas, and Zachary Cohen, "Georgia Election Official Says Battleground State Fended Off Cyberattack Likely From a Foreign Country," *CNN*, October 23, 2024. (https://www.cnn.com/2024/10/23/politics/georgia-election-official-cyber-attack/index.html)

states,[3] although Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency (CISA), cautioned that the email addresses alone do not necessarily implicate the Russian government.[4]

Despite all these efforts, foreign malign influence campaigns failed to achieve measurable results. Truly assessing the impact of foreign malign influence remains challenging: even content that goes viral may not affect the viewer, and researchers may have missed operations sophisticated enough to avoid detection.[5] But without question, in the year leading up to the 2024 U.S. elections, researchers exposed many operations before their content gained traction, and the U.S. government expeditiously exposed content from foreign influence campaigns that did in fact gain significant reach. And while Russia, Iran, and China all integrated artificial intelligence into their operations, this did not create more persuasive disinformation but rather seemed to help scale content that was often of low quality.

American society has made tremendous progress in combating foreign malign influence since 2016, when Russia's aggressive cyber-enabled influence operations caught many Americans off guard.[6] This success, however, should not lull the public into a sense of complacency. Rather, it should inform and motivate stakeholders throughout American society to continue researching, monitoring, and combating foreign malign influence operations. Letting up on the gas only risks making the American people more susceptible to future attacks.

Russia

On multiple occasions prior to Election Day, the U.S. government warned that Russia's malign influence presented the most significant threat to U.S. elections.[7] And indeed, Moscow was the most aggressive active threat actor. Overall, at least six separate Russian operations targeted the 2024 U.S. elections, as detailed below. These operations displayed distinct tactics, techniques, and procedures (TTPs) and involved distinct operators (that is, where operators have been identified), but they sometimes amplified each other's content.[8]

3. Tim Reid and Sarah N. Lynch, "Hoax Bomb Threats Linked to Russia Target Polling Places in Battleground States, FBI Says," *Reuters*, November 5, 2024. (https://www.reuters.com/world/us/fake-bomb-threats-linked-russia-briefly-close-georgia-polling-locations-2024-11-05)
4. Martin Matishak, "Top US Cyber Official Says 'No Evidence of Malicious Activity' Impacting Election," *The Record*, November 6, 2024. (https://therecord.media/cisa-easterly-no-evidence-of-malicious-election-activity)
5. Jon Bateman, Elonnai Hickok, Laura Courchesne, Isra Thange, and Jacob N. Shapiro, "Measuring the Effects of Influence Operations: Key Findings and Gaps From Empirical Research," *Carnegie Endowment for International Peace*, June 28, 2021. (https://carnegieendowment.org/research/2021/06/measuring-the-effects-of-influence-operations-key-findings-and-gaps-from-empirical-research)
6. Martin Matishak, "Senate Intelligence Report on Russian Meddling Sounds Alarm for 2020," *Politico*, July 25, 2019. (https://www.politico.com/story/2019/07/25/russia-interference-2016-election-1435436); Tim Starks, Laurens Cerulus, and Mark Scott, "Russia's Manipulation of Twitter Was Far Vaster Than Believed," *Politico*, June 5, 2019. (https://www.politico.com/story/2019/06/05/study-russia-cybersecurity-twitter-1353543)
7. U.S. Office of the Director of National Intelligence, Press Release, "100 Days Until Election 2024: Election Security Update as of Late-July 2024," July 29, 2024. (https://www.dni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240729.pdf); U.S. Office of the Director of National Intelligence, Press Release, "60 Days Until Election 2024: Election Security Update as of Early September 2024," September 6, 2024. (https://www.dni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240906.pdf)
8. Max Lesser, "Foreign Malign Election Meddling Persists But Struggles to Gain Traction," *Foundation for Defense of Democracies*, October 29, 2024. (https://www.fdd.org/wp-content/uploads/2024/10/fdd-memo-foreign-malign-election-meddling-persists-but-struggles-to-gain-traction.pdf)

CopyCop

CopyCop, also known as Storm-1516 and the John Mark Dougan Network, had the greatest success in reaching mass audiences.[9] Several of CopyCop's videos advancing false claims about Harris and Governor Tim Walz went viral, but researchers and the U.S. government exposed and debunked the claims.[10] Clemson University first exposed the network, and the cybersecurity company Recorded Future subsequently published research uncovering vast networks of fake websites and the techniques CopyCop used to create them.[11]

John Mark Dougan, a former American police officer who now resides in Russia, orchestrated CopyCop. Dougan allegedly liaised directly with a senior figure in a political warfare unit of Russia's military intelligence and receives funding and direction from a Kremlin-linked organization.[12] Dougan's network also reportedly has historical, technical, and organizational ties to the Foundation to Battle Injustice, discussed below.[13] Between May and June of 2024, CopyCop shifted its focus from the war in Ukraine toward primarily pushing U.S. election-related content, though it also continued publishing content about Ukraine, other European countries, and Israel.[14]

In addition to videos, Dougan created over 160 fake websites with the help of commercial artificial intelligence (AI) tools such as ChatGPT and DALL-E 3.[15] CopyCop's websites sometimes assumed novel domain names and sometimes imitated defunct U.S. media outlets.[16] CopyCop's websites often plagiarized articles using generative AI to rewrite content sourced from Russian media, conservative American media, and mainstream British and French media.

CopyCop's election-related content often promoted outlandish narratives about Harris and Walz.[17] In addition, Copycop attempted to erode Americans' faith in the integrity of the Intelligence Community while also stirring

9. Different research organizations often give different names to the same operation. For example, Recorded Future refers to John Mark Dougan's network as "CopyCop," while Microsoft refers to it as "Storm-1516." In this report, FDD provides all the available names to aid readers in identifying the operations.
10. U.S. Office of the Director of National Intelligence, Press Release, "45 Days Until Election 2024: Election Security Update as of Mid-September 2024," September 23, 2024. (https://www.odni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240923.pdf)
11. Insikt Group, "Russia-Linked CopyCop Uses LLMs to Weaponize Influence Content at Scale," *Recorded Future*, May 9, 2024. (https://go.recordedfuture.com/hubfs/reports/cta-2024-0509.pdf)
12. Catherine Belton, "American Creating Deepfakes Targeting Harris Works With Russian Intel, Documents Show," *The Washington Post*, October 23, 2024. (https://www.washingtonpost.com/world/2024/10/23/dougan-russian-disinformation-harris)
13. Patrick Warren and Darren Linvill, "Writers of the Storm: Who's Behind the Ongoing Production of Pro-Russian False Narratives," *Clemson University Media Forensics Hub*, October 2024. (https://open.clemson.edu/cgi/viewcontent.cgi?article=1009&context=mfh_ci_reports)
14. Insikt Group, "Russia-Linked CopyCop Expands to Cover U.S. Elections, Target Political Leaders," *Recorded Future*, June 24, 2024. (https://go.recordedfuture.com/hubfs/reports/cta-ru-2024-0624.pdf)
15. Steven Lee Myers, "Once a Sheriff's Deputy in Florida, Now a Source of Disinformation From Russia," *The New York Times*, May 29, 2024. (https://www.nytimes.com/2024/05/29/business/mark-dougan-russia-disinformation.html)
16. Insikt Group, "Russia-Linked CopyCop Uses LLMs to Weaponize Influence Content at Scale," *Recorded Future*, May 9, 2024. (https://go.recordedfuture.com/hubfs/reports/cta-2024-0509.pdf); Insikt Group, "Russia-Linked CopyCop Expands to Cover U.S. Elections, Target Political Leaders," *Recorded Future*, June 24, 2024. (https://go.recordedfuture.com/hubfs/reports/cta-ru-2024-0624.pdf)
17. "Russia Leverages Cyber proxies and Volga Flood Assets in Expansive Influence Efforts," *Microsoft Threat Analysis Center*, September 17, 2024, page 2. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-4.pdf); "Lead-up to Election Day 2024: Russia, Iran, and China Engaging in Influence Activity in Final Weeks Before Election Day 2024," *Microsoft Threat Analysis Center*, October 23, 2024, pages 4-5. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-5-on-Russian-Influence.pdf)

up resentment toward Ukraine. For example, CopyCop claimed that the CIA ordered a Ukrainian troll farm to interfere in the election, that the FBI wiretapped Trump, and that Ukrainian soldiers burned an effigy of Trump.[18]

To promote its narratives, CopyCop often used paid actors posing as journalists or whistleblowers.[19] CopyCop then used its network of fake websites and social media accounts to amplify interviews with these paid actors. These narratives spread on X, Telegram, and YouTube, and domains associated with the Russian influence operations Doppelganger and Portal Kombat (discussed below) also shared content from CopyCop on their own websites.[20]

Operation Overload

Operation Overload, also known as Matryoshka and Storm-1679, spread false claims on Telegram and X.[21] The operation's distinctive feature is its efforts to send requests to fact-checkers, media organizations, and journalists to debunk these false claims.[22] In addition to overloading the capacity of fact-checkers and journalists, the campaign sought to have fact-checkers and journalists debunk the narratives publicly so that Kremlin-aligned narratives could gain additional visibility. While the operation historically pushed anti-Ukraine narratives and targeted the Paris Olympics, the operation largely shifted its focus to U.S. elections around September 2024.

Operation Overload often imitated reputable brands and organizations. Its fake Instagram stories, for example, imitated Instagram accounts from CNN, Fox, The New York Times, and the New York Post.[23] In the operation's X posts, it often shared videos imitating legitimate news outlets such as the BBC by using their logos and imitating their design and layout.[24]

The operation also sought to influence audiences directly by spreading claims through inauthentic accounts on X. Those posts often included QR codes that linked to official websites of government agencies, such as the French

18. "Iran Steps Into U.S. Election 2024 With Cyber-Enabled Influence Operations," *Microsoft Threat Analysis Center*, August 9, 2024, page 5. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf)

19. Ibid.

20. "Lead-up to Election Day 2024: Russia, Iran, and China Engaging in Influence Activity in Final Weeks Before Election Day 2024," *Microsoft Threat Analysis Center*, October 23, 2024. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-5-on-Russian-Influence.pdf); "Russia Leverages Cyber proxies and Volga Flood Assets in Expansive Influence Efforts," *Microsoft Threat Analysis Center*, September 17, 2024. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-4.pdf); "Investigation: Chinese Bot Network Is Amplifying Russian Disinformation About the U.S. Election," *Digital Forensic Research Lab*, November 5, 2024. (https://dfrlab.org/2024/11/05/russia-china-us-election-operation-overload); Insikt Group, "Operation Overload Impersonates U.S. Media to Influence 2024 U.S. Election," *Recorded Future*, October 23, 2024. (https://go.recordedfuture.com/hubfs/reports/ta-ru-2024-1023.pdf)

21. Théo Marie-Courtois and Juliette Mansour, "'Matriochka,' La Nouvelle Campagne de Désinformation Anti-Ukrainienne à Destination des Médias Occidentaux ['Matryoshka,' The New Anti-Ukrainian Disinformation Campaign Aimed at Western Media]," *Agence France-Presse* (France), January 30, 2024. (https://factuel.afp.com/doc.afp.com.34H32VP); CheckFirst and Reset.Tech, "Operation Overload," June 2024. (https://checkfirst.network/wp-content/uploads/2024/06/Operation_Overload_WEB.pdf)

22. CheckFirst and Reset.Tech, "Operation Overload," June 2024. (https://checkfirst.network/wp-content/uploads/2024/06/Operation_Overload_WEB.pdf); CheckFirst, "Operation Overlord: Activity Update - September 2024," September 12, 2024. (https://checkfirst.network/wp-content/uploads/2024/09/Operation_Overload_Activity_Update_September_2024.pdf)

23. CheckFirst, "Operation Overlord: Activity Update - September 2024," September 12, 2024. (https://checkfirst.network/wp-content/uploads/2024/09/Operation_Overload_Activity_Update_September_2024.pdf); Insikt Group, "Operation Overload Impersonates U.S. Media to Influence 2024 U.S. Election," *Recorded Future*, October 23, 2024. (https://go.recordedfuture.com/hubfs/reports/ta-ru-2024-1023.pdf)

24. "Operation Overload Impersonates U.S. Media to Influence 2024 U.S. Election," *Recorded Future*, October 23, 2024. (https://go.recordedfuture.com/hubfs/reports/ta-ru-2024-1023.pdf)

counter-foreign malign influence agency VIGINUM as well as mainstream media organizations.[25] Recorded Future also found that for several of the operation's QR codes, files would download onto a user's computer when he or she opened the QR code. While Recorded Future determined the payloads to be benign, malicious actors can use QR codes to trick victims into installing malware.[26]

The operation also used AI-generated voiceovers to fabricate content, sometimes using AI to create a generic broadcaster's voice. Notably, Operation Overload used AI to imitate the voice of FBI Director Chris Wray to depict him making fabricated claims of voter fraud.[27]

Operation Overload's election-related content criticized both Harris and Trump, but Recorded Future found that anti-Harris content outnumbered anti-Trump content by four to one.[28] The operation also attempted to stoke fear of post-election political violence or civil war, denigrate Ukrainian refugees in the United States, and provoke anti-LGBT sentiment. It also sought to advance claims of voter fraud in the days leading up to the elections, often using the logos of the FBI and Voice of America in social media posts. Pro-Kremlin influencers and other Russian influence operations, such as Portal Kombat, also amplified Operation Overload's content.

Operation Overload's social media posts do not appear to have garnered significant organic engagement. They did, however, trick fact-checking organizations into spreading their narratives over 250 times, thus injecting these narratives into the broader information ecosystem.[29]

Doppelganger

Doppelganger, also known as Ruza Flood and Storm-1099, started pushing polarizing content related to the 2024 U.S. elections as early as November 2023, when the domain electionwatch[.]live began criticizing President Joe Biden's economic, social, and security policies and noting his declining favorability among Black voters.[30] Over the years, many researchers have reported on Doppelganger's activity,[31] and in September 2024, the Department of Justice (DOJ) seized over 32 domains associated with the operation.[32] The prior March, the Treasury Department sanctioned the heads of the two companies that run Doppelganger, confirming that they acted "at the direction

25. CheckFirst, "Operation Overlord: Activity Update - September 2024," September 12, 2024. (https://checkfirst.network/wp-content/uploads/2024/09/Operation_Overload_Activity_Update_September_2024.pdf)
26. Insikt Group, "Operation Overload Impersonates U.S. Media to Influence 2024 U.S. Election," *Recorded Future*, October 23, 2024. (https://go.recordedfuture.com/hubfs/reports/ta-ru-2024-1023.pdf)
27. Insikt Group, "Operation Overload Impersonates U.S. Media to Influence 2024 U.S. Election," *Recorded Future*, October 23, 2024. (https://go.recordedfuture.com/hubfs/reports/ta-ru-2024-1023.pdf); "Investigation: Chinese Bot Network Is Amplifying Russian Disinformation About the U.S. Election," *Digital Forensic Research Lab*, November 5, 2024. (https://dfrlab.org/2024/11/05/russia-china-us-election-operation-overload)
28. Ibid.
29. Ibid.
30. Insikt Group, "Obfuscation and AI Content in the Russian Influence Network 'Doppelgänger' Signals Evolving Tactics," *Recorded Future*, December 5, 2023. (https://go.recordedfuture.com/hubfs/reports/ta-2023-1205.pdf)
31. EU Disinfo Lab, "What is the Doppelganger Operation? List of Resources," October 30, 2024. (https://www.disinfo.eu/doppelganger-operation)
32. U.S. Department of Justice, Office of Public Affairs, Press Release, "Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere," September 4, 2024. (https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence).

of the Russian Presidential Administration."[33] Though the Doppelganger campaign proved persistent, available evidence suggests its election-related content did not receive significant engagement from authentic users.[34]

Doppelganger's behavior generally incorporates two primary techniques: first creating fake websites imitating major news outlets such as Fox News and The Washington Post, then disseminating links to these websites via inauthentic social media accounts. To trick viewers into believing they are on the actual news outlet's website, Doppelganger imitates the legitimate website's logos, layout, and design. It also imitates their domain names, using, for example, washingtonpost[.]pm to mimic washingtonpost[.]com.[35] This technique is known as "typosquatting."

Once Doppelganger created these phony news websites, it used inauthentic social media accounts to promote the content. The campaign employed multiple sophisticated techniques to avoid detection by social media platforms. For example, when Meta began blocking domains associated with Doppelganger, the operation began to circumvent Meta's efforts by sharing links that redirect multiple times before eventually landing on a Doppelganger domain.[36] In some instances, Doppelganger also used cloaking services that would redirect target audiences to Doppelganger websites while redirecting moderators to benign websites.[37] Like many malicious cyber and influence campaigns, Doppelganger sometimes accessed web hosting servers through "bulletproof" hosting providers, which are internet infrastructure companies that typically refuse to cooperate with law enforcement.[38]

33. U.S. Department of the Treasury, Press Release, "Treasury Sanctions Actors Supporting Kremlin-Directed Malign Influence Efforts," March 20, 2024. (https://home.treasury.gov/news/press-releases/jy2195); EU Disinfo Lab, "What is the Doppelganger Operation? List of Resources," October 30, 2024. (https://www.disinfo.eu/doppelganger-operation). Note: While the Treasury press release does not specifically call out Doppelganger, researchers have linked Doppelganger to the companies associated with the individuals sanctioned by Treasury.

34. Sekoia TDR, Coline Chavane, Amaury G., and Kilian Seznec, "Master of Puppets: Uncovering the DoppelGänger Pro-Russian Influence Campaign," *Sekoia*, May 21, 2024. (https://web.archive.org/web/20240521180803/https://blog.sekoia.io/master-of-puppets-uncovering-the-doppelganger-pro-russian-influence-campaign); Insikt Group, "Obfuscation and AI Content in the Russian Influence Network 'Doppelgänger' Signals Evolving Tactics, *Recorded Future*, December 5, 2023. (https://go.recordedfuture.com/hubfs/reports/ta-2023-1205.pdf)

35. Ben Nimmo, Nathaniel Gleicher, Margarita Franklin, Lindsay Hundley, and Mike Torrey, "Third Quarter Adversarial Threat Report," *Meta*, November 2023. (https://web.archive.org/web/20241205154209/https://scontent-lax3-1.xx.fbcdn.net/v/t39.8562-6/406961197_3573768156197610_1503341237955279091_n.pdf?_nc_cat=105&ccb=1-7&_nc_sid=b8d81d&_nc_ohc=W-nmDdyX2MkQ7kNvgFEgogG&_nc_zt=14&_nc_ht=scontent-lax3-1.xx&_nc_gid=ANyIznSrWGrMi2lYwOn632g&oh=00_AYByVhFZiRshbGmI_jRUmZgjviVppZdXT0yMMPVpDoVRQQ&oe=6757AA52); U.S. Department of Justice, Office of Public Affairs, Press Release, "Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere," September 4, 2024. (https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence)

36. "How Russia Uses EU Companies for Propaganda," *Qurium*, July 11, 2024. (https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/#FIKED); Ben Nimmo, Mike Torrey, Margarita Franklin, David Agranovich, Margie Milam, Lindsay Hundley, and Robert Flaim, "Second Quarter Adversarial Threat Report," *Meta*, December 3, 2024. (https://transparency.meta.com/metasecurity/threat-reporting); "When Kehr Meets Vextrio," *Qurium*, November 13, 2024. (https://www.qurium.org/forensics/when-kehr-meets-vextrio)

37. European Digital Media Observatory, "Doppelganger: CORRECTIV Investigations Bring Russian Propaganda Campaign to a Halt," November 18, 2024. (https://edmo.eu/publications/doppelganger-correctiv-investigations-bring-russian-propaganda-campaign-to-a-halt); "When Kehr Meets Vextrio," *Qurium*, November 13, 2024. (https://www.qurium.org/forensics/when-kehr-meets-vextrio); Alexandre Alaphilippe, Gary Machado, Raquel Miguel, and Francesco Poldi, "Doppelganger: Media Clones Serving Russian Propaganda," (https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf); Ben Nimmo, Margarita Franklin, David Agranovich, Lindsay Hundley, and Mike Torrey, "Quarterly Adversarial Threat Report," February 2023. (https://about.fb.com/wp-content/uploads/2023/02/Meta-Quarterly-Adversarial-Threat-Report-Q4-2022.pdf)

38. "How Russia Uses EU Companies for Propaganda," *Qurium*, July 11, 2024. (https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/#FIKED)

By early 2024, at least 15 Doppelganger domains were publishing content about the election, continuing to criticize Biden, Harris, Walz, and the Democratic Party.[39] After the July 13 attempted assassination of Trump, Doppelganger domains portrayed the former president as a martyr and suggested that the Democratic Party perpetrated the assassination attempt, a narrative further spread by Russian officials and vloggers.[40] FDD also analyzed a set of Doppelganger-related posts on X in partnership with the Counter Disinformation Network and found that many Doppelganger accounts attacked Democratic candidates as a vehicle for undermining U.S. support for Ukraine, and vice versa.[41]

Although social media companies generally took down Doppelganger accounts quickly, the operation persisted because its operators quickly created new fake websites and acquired new inauthentic accounts.[42] In the words of Meta's threat researchers, Doppelganger has been as "persistent and voluminous in its attempts as spammers are in targeting people online with knockoff merchandise: constantly shifting key words, spelling, off-platform links, and images, and churning through many burner accounts and [Facebook] Pages to only leave a single comment or run a single ad before we block them."[43]

Doppelganger also quickly recreated websites taken down by DOJ. The Atlantic Council's Digital Forensic Research Lab found that Doppelganger recreated many of its websites within 24 hours.[44] Doppelganger would simply recreate the website with a new top-level domain. For example, after the FBI seized 50statesoflie[.]media, Doppelganger

39. Esteban Ponce de León, "Doppelganger Websites Persist One Month Following U.S. Government Seizures," *Digital Forensic Research Lab*, October 9, 2024. (https://dfrlab.org/2024/10/09/doppelganger-websites-persist); Insikt Group, "Malign Influence Threats Mount Ahead of U.S. 2024 Elections," *Recorded Future*, August 13, 2024. (https://go.recordedfuture.com/hubfs/reports/ta-2024-0813.pdf)

40. Sopo Gelava and Ruslan Trad, "How Pro-Kremlin Influencers Spread Unfounded Connections Between Ukraine and a Would-Be Trump Assassin," *Digital Forensic Research Lab*, September 23, 2024. (https://dfrlab.org/2024/09/23/routh-conspiracy-theories-russia)

41. Max Lesser and RADM (Ret.) Mark Montgomery, "How U.S. Adversaries Undermine the Perception of Election Integrity," *Foundation for Defense of Democracies*, September 26, 2024. (https://www.fdd.org/analysis/2024/09/26/how-u-s-adversaries-undermine-the-perception-of-election-integrity)

42. Lea Früwirth and Saman Nazari (Eds.), "Fool Me Once: Russian Influence Operation Doppelganger Continues on X and Facebook," *Alliance4Europe*, September 2024. (https://alliance4europe.eu/wp-content/uploads/2024/09/CDN-Report-%E2%80%93-Fool-Me-Once_-Russian-Influence-Operation-Doppelganger-Continues-on-X-and-Facebook-%E2%80%93-September-2024.pdf); Margarita Franklin, Lindsay Hundley, Mike Torrey, David Agranovich, and Mike Dvilyanski, "First Quarter Adversarial Threat Report," *Meta*, May 2024. (https://web.archive.org/web/20241205161414/https://scontent-lax3-2.xx.fbcdn.net/v/t39.8562-6/445235204_402858536059630_7403303878106178024_n.pdf?_nc_cat=100&ccb=1-7&_nc_sid=b8d81d&_nc_ohc=txVRSj9tBwoQ7kNvgEaGt4T&_nc_zt=14&_nc_ht=scontent-lax3-2.xx&_nc_gid=A9S1H4KFjM6M5xbAiv-IZCp&oh=00_AYBgzCB0xZ470HBOCuKojqY4_jtl_5TmoGLGWv13rvt0kA&oe=675799FF)

43. Margarita Franklin, Lindsay Hundley, Mike Torrey, David Agranovich, and Mike Dvilyanski, "First Quarter Adversarial Threat Report," *Meta*, May 2024. (https://web.archive.org/web/20241205161414/https://scontent-lax3-2.xx.fbcdn.net/v/t39.8562-6/445235204_402858536059630_7403303878106178024_n.pdf?_nc_cat=100&ccb=1-7&_nc_sid=b8d81d&_nc_ohc=txVRSj9tBwoQ7kNvgEaGt4T&_nc_zt=14&_nc_ht=scontent-lax3-2.xx&_nc_gid=A9S1H4KFjM6M5xbAiv-IZCp&oh=00_AYBgzCB0xZ470HBOCuKojqY4_jtl_5TmoGLGWv13rvt0kA&oe=675799FF)

44. Esteban Ponce de León, "Doppelganger Websites Persist One Month Following U.S. Government Seizures," *Digital Forensic Research Lab*, October 9, 2024. (https://dfrlab.org/2024/10/09/doppelganger-websites-persist)

quickly recreated the website with the domain name 50statesoflie[.]so. FDD also identified two new Doppelganger domains recreated with the same pattern, tribunalukraine[.]org and lexomnium[.]pw.[45]

Other Russian Operations

While CopyCop, Operation Overload, and Doppelganger are the most widely reported Russian influence operations that targeted the 2024 U.S. elections, several other Russian operations also targeted the elections, including Portal Kombat, Volga Flood, and others.

French agency VIGINUM first exposed Portal Kombat in February 2024, describing it as a "structured and coordinated pro-Russian propaganda network."[46] FDD and other researchers observed Portal Kombat's English-language domains posting a high volume of election-related content, typically pro-Trump and anti-Harris.[47] FDD also observed the creation of a Pravda domain, pravda-us[.]online, which appeared almost entirely dedicated to U.S. issues. The domain prominently featured topics related to the 2024 U.S. elections, with dedicated tabs for Trump, Harris, and Biden.[48]

Several operations associated with the late Russian businessman Yevgeniy Prigozhin, the notorious founder of the Wagner paramilitary group and the Internet Research Agency troll farm, continued to launch malign influence campaigns even after Prigozhin's death in August 2023. The Russian media organization Rybar, which Microsoft refers to as Storm-1841 or Volga Flood,[49] created multiple inauthentic Telegram channels and X accounts not in its

45. "Tribunalukraine[.]org – Whois," *Whoxy*, accessed October 15, 2024. (https://www.whoxy.com/tribunalukraine.org); "Lexomnium[.]pw – Whois," *Whoxy*, accessed October 15, 2024. (https://www.whoxy.com/lexomnium.pw); "20% der Ukrainer Sind Nazis? [20% of Ukrainians are Nazis?]," *Tribunal Ukraine* (Russia), accessed October 15, 2024. (https://ghostarchive.org/archive/B5MlX); "Die Regierung Biden Hat dem Kongress einen Geheimen Bericht über die Korruption in der Ukraine Vorgelegt [The Biden Administration Has Submitted a Secret Report to Congress on Corruption in Ukraine], *Tribunal Ukraine* (Russia), accessed October 15, 2024. (https://ghostarchive.org/archive/hZL5Y); "Ukrainische Soldaten Sind in SS-Uniformen in die Region Kursk Eingedrungen [Ukrainian Soldiers in SS Uniforms Invaded the Kursk Region], *Tribunal Ukraine* (Russia), accessed October 15, 2024. (https://ghostarchive.org/archive/jebBd); "Les États-Unis Obligent l'Europe à Soutenir Financièrement l'Ukraine [The United States Forces Europe to Financially Support Ukraine]," *Lex Omnium* (Russia), October 11, 2024. (https://ghostarchive.org/archive/CTvJ9); "Mercenaires et Armes : l'Ukraine Vole les Ressources de l'Europe [Mercenaries and Weapons: Ukraine Steals Europe's Resources]," *Lex Omnium* (Russia), October 9, 2024. (https://ghostarchive.org/archive/NUgPp); "Flambée des Crimes de Haine dans les Écoles: Le Gouvernement Incapable de Freiner la Radicalisation Croissante [Surge in Hate Crimes in Schools: Government Unable to Curb Growing Radicalization]," *Lex Omnium* (Russia), October 3, 2024. (https://ghostarchive.org/archive/I3MJw)

46. VIGINUM, "PORTAL KOMBAT: A Structured and Coordinated Pro-Russian Propaganda Network," February 2024. (https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf)

47. Max Lesser, "Foreign Malign Election Meddling Persists But Struggles to Gain Traction," *Foundation for Defense of Democracies*, October 29, 2024. (https://www.fdd.org/analysis/2024/10/29/foreign-malign-election-meddling-persists-but-struggles-to-gain-traction); Insikt Group, "Russia-Linked CopyCop Uses LLMs to Weaponize Influence Content at Scale," *Recorded Future*, May 9, 2024. (https://go.recordedfuture.com/hubfs/reports/cta-2024-0509.pdf); Insikt Group, Operation Overload Impersonates Media to Influence 2024 U.S. Election," *Recorded Future*, October 23, 2024. (https://go.recordedfuture.com/hubfs/reports/ta-ru-2024-1023.pdf)

48. Max Lesser, "Foreign Malign Election Meddling Persists But Struggles to Gain Traction," *Foundation for Defense of Democracies*, October 29, 2024. (https://www.fdd.org/analysis/2024/10/29/foreign-malign-election-meddling-persists-but-struggles-to-gain-traction)

49. U.S. Department of State, Rewards for Justice, "Rybar Employees," accessed December 5, 2024. (https://rewardsforjustice.net/rewards/rybar); "Russia Leverages Cyber proxies and Volga Flood Assets in Expansive Influence Efforts," *Microsoft Threat Analysis Center*, September 17, 2024, page 2. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-4.pdf)

own name that shared polarizing content in attempts to divide Americans and even encourage acts of violence.[50] One of Rybar's lead authors used to serve in the press office of the Russian Ministry of Defense.[51] Prigozhin had once funded Rybar, and Rybar also receives funding from state-owned Rostec, Russia's main military-industrial conglomerate, which is under U.S. sanctions. In October 2024, the State Department released a Rewards for Justice offering money in exchange for information about Rybar, citing its activities targeting American audiences in advance of the 2024 elections.[52]

The Newsroom for American and European Based Citizens — also once financed by Prigozhin — pushed content criticizing Biden, supporting Trump, and promoting claims of election fraud on the social media platform Gab.[53] Similarly, a Russian nonprofit organization known as the Foundation to Battle Injustice, also previously financed by Prigozhin, pushed numerous outlandish claims about Harris and Walz. In addition, it promoted conspiracy theories alleging that the Biden administration would launch a false flag cyberattack on Election Day and that the Democratic Party would engage in widespread voter fraud.[54] The Foundation to Battle Injustice also alleged that the Pentagon authorized U.S. military personnel to use lethal force against Americans and that the Democratic Party planned to assassinate GOP leaders with the assistance of the Intelligence Community.[55]

Iran and Its Proxies

Iran punched above its weight this election cycle, distinguishing itself by launching aggressive cyber-enabled influence operations targeting the Trump campaign. In addition, Iran also conducted conventional online influence operations leveraging inauthentic social media accounts and news websites, several of which targeted specific demographics and regions.

50. "Iran Steps Into U.S. Election 2024 With Cyber-Enabled Influence Operations," *Microsoft Threat Analysis Center*, August 9, 2024, page 5. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf)

51. Irina Pankratova, "Создатель «Рыбаря». Продолжение расследования The Bell [The creator of 'Rybar'. The Bell's investigation continues]," *The Bell*, November 19, 2022. (https://thebell.io/sozdatel-rybarya-prodolzhenie-rassledovaniya-the-bell)

52. U.S. Department of State, Rewards for Justice, "Rybar Employees," accessed December 5, 2024. (https://rewardsforjustice.net/rewards/rybar)

53. Insikt Group, "Malign Influence Threats Mount Ahead of U.S. 2024 Elections," *Recorded Future*, August 13, 2024. (https://go.recordedfuture.com/hubfs/reports/ta-2024-0813.pdf); Alden Wahlstrom, David Mainor, and Daniel Kapellmann Zafra, "Life After Death? IO Campaigns Linked to Notorious Russian Businessman Prigozhin Persist After His Political Downfall and Death," *Mandiant*, March 28, 2024. (https://cloud.google.com/blog/topics/threat-intelligence/io-campaigns-russian-prigozhin-persist)

54. "The Biden Administration Is Preparing a False-Flag Cyberattack in the U.S. to Rig the Election in Favor of Kamala Harris," *Foundation to Battle Injustice*, October 30, 2024. (https://web.archive.org/web/20241127151315/https://fondfbr.ru/en/articles/cyber-attack-us-election-for-harris-en); "The Biden-Harris Administration Is Plotting a Massive Voter Fraud Scheme for the U.S. Presidential Election," *Foundation to Battle Injustice*, November 1, 2024. (https://web.archive.org/web/20241127151613/https://fondfbr.ru/en/articles/democrats-dirty-election-tactics-en); "The Foundation to Battle Injustice Has Obtained Evidence of Democratic Plans to Rig the Presidential Election in a Key Swing State," *Foundation to Battle Injustice*, November 3, 2024. (https://web.archive.org/web/20241127151138/https://fondfbr.ru/en/articles/arizona-elections-fraud-en); Max Lesser, "Foreign Malign Election Meddling Persists But Struggles to Gain Traction," *Foundation for Defense of Democracies*, October 29, 2024. (https://www.fdd.org/analysis/2024/10/29/foreign-malign-election-meddling-persists-but-struggles-to-gain-traction)

55. "Biden-Harris Regime Authorizes Law Enforcement Killings of Americans Under 'Special Circumstances'," *Foundation to Battle Injustice*, October 11, 2024. (https://web.archive.org/web/20241127152746/https://fondfbr.ru/en/articles/biden-harris-assassinate-american-citizens-en); "Democrats and U.S. Security Services Are Preparing Mass Assassinations of MAGA Movement Leaders Shortly After the 2024 U.S. Elections," *Foundation to Battle Injustice*, October 22, 2024. (https://web.archive.org/web/20241127152348/https://fondfbr.ru/en/articles/us-intelligence-democrats-against-maga-en)

An English-language operation seemingly conducted by Iranian proxy Hezbollah also appears to have attempted to undermine Americans' faith in election integrity, in addition to criticizing Israel. However, after Israel invaded southern Lebanon on October 1, 2024, nearly a year after Hezbollah initiated the most recent round of fighting, the operation shifted its focus almost entirely to criticizing Israel.

APT-42

Led by APT-42, also known as Mint Sandstorm and UNC788, Iran conducted aggressive cyber-enabled influence operations targeting U.S. political campaigns. Cyber threat researchers have previously linked APT-42 to Iran's Islamic Revolutionary Guard Corps (IRGC). APT-42 is known for cyberattacks against individuals and organizations involved in foreign policy and politics in America, Israel, and other regions of interest to Iran.[56]

Microsoft first reported APT-42's election-related activity on August 9, 2024, noting that the group targeted a senior official of an unspecified presidential campaign with a spear-phishing email sent from the compromised email account of a former senior advisor to the candidate.[57] Less than a week later, Google reported that APT-42 had targeted officials associated with both the Biden and Trump campaigns in May and June of 2024, observing that APT-42 successfully breached a high-profile political consultant's Gmail account.[58] Later in August, Meta reported that it disrupted APT-42's social engineering activity on WhatsApp.[59]

Neither Microsoft nor Google specified which senior advisor or high-profile political consultant APT-42 successfully compromised, and it is not clear whether they are referring to the same individual in their respective reports. Media outlets, including CNN and The Washington Post, however, reported separately that Iranian threat actors breached Roger Stone's email account and used it to reach out to other Trump campaign officials.[60]

APT-42 successfully exfiltrated sensitive Trump campaign documents, including opposition research on then vice presidential candidate JD Vance.[61] APT-42 first sent excerpts of the documents to officials affiliated with the Biden campaign in June and July 2024 in an attempt to have them published — but to no avail.[62] The same operatives then sent the documents to mainstream outlets, including Politico, hoping the news outlets would publish the

56. Ofir Rozmann, Asli Koksal, Adrian Hernandez, Sarah Bock, and Jonathan Leathery, "Uncharmed: Untangling Iran's APT42 Operations," *Mandiant*, May 1, 2024. (https://cloud.google.com/blog/topics/threat-intelligence/untangling-iran-apt42-operations); Threat Analysis Group, "Iranian Backed Group Steps Up Phishing Campaigns Against Israel, U.S.," *Google*, August 14, 2024. (https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us)

57. "Iran Steps Into U.S. Election 2024 With Cyber-Enabled Influence Operations," *Microsoft Threat Analysis Center*, August 9, 2024. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf)

58. Threat Analysis Group, "Iranian Backed Group Steps Up Phishing Campaigns Against Israel, U.S.," *Google*, August 14, 2024. (https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us)

59. "Taking Action Against Malicious Accounts in Iran," *Meta*, August 23, 2024. (https://about.fb.com/news/2024/08/taking-action-against-malicious-accounts-in-iran)

60. Adam Gabbatt, "Roger Stone's Email Account Breached by Alleged Iranian Hackers," *The Guardian* (UK), August 13, 2024. (https://www.theguardian.com/us-news/article/2024/aug/13/roger-stone-email-hack-iran-trump)

61. Christopher Bing, Raphael Satter, and Gram Slattery, "Exclusive: Accused Iranian Hackers Successfully Peddle Stolen Trump Emails," *Reuters*, October 25, 2024. (https://www.reuters.com/world/us/accused-iranian-hackers-successfully-peddle-stolen-trump-emails-2024-10-25)

62. U.S. Office of the Director of National Intelligence, "Joint ODNI, FBI, and CISA Statement," September 18, 2024. (https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2024/3994-odni-pr-22)

documents.[63] No mainstream media outlets took the bait, but a Democratic political operative and an independent journalist did share the material online.[64] The FBI responded by indicting three individuals allegedly involved in Iran's malicious cyber activity. While it does not specifically name APT-42, the indictment describes activity matching that reported by Microsoft and Google, and Reuters reported that the indictment targeted APT-42.[65]

Inauthentic News Websites

Iran also created a network of fake websites posing as American news outlets to target American voters along demographic, regional, and ideological lines in advance of the 2024 U.S. elections. Microsoft first reported on the domains in this network in August 2024, referring to the operators as Storm-2035. OpenAI later identified several other domains in the network. Notably, OpenAI reported that it banned several ChatGPT accounts for using its model to generate long-form articles for the domains as well as social media comments in English and Spanish promoting the network.[66]

FDD identified still more domains targeting the U.S. elections, discovering that this network is part of a broader network of at least 19 domains targeting foreign audiences. These domains shared common hosting infrastructure and other technical indicators.[67] A total of eight domains from this operation targeted the 2024 U.S. elections, namely niothinker[.]com, evenpolitics[.]com, westlandsun[.]com, afromajority[.]com, savannahtime[.]com, teorator[.]com, notourwar[.]com, and lalinearoja[.]net. Most of these domains typically praised Harris and criticized Trump, but several others supported Trump.[68] The variety in the narratives promoted by these websites — some progressive, some conservative — indicates that while other Iranian operations sought to denigrate the Trump campaign, this network sought to deepen political polarization in the United States.

Bushnell's Men

Bushnell's Men, an Iranian influence operation first exposed by Microsoft, also targeted the 2024 U.S. elections.[69] The operation takes its name from Aaron Bushnell, a 25-year-old U.S. Air Force service member who self-immolated

63. Alex Isenstadt, "We Received Internal Trump Documents from 'Robert.' Then the Campaign Confirmed It Was Hacked." *Politico*, August 10, 2024. (https://www.politico.com/news/2024/08/10/trump-campaign-hack-00173503)
64. Christopher Bing, Raphael Satter, and Gram Slattery, "Exclusive: Accused Iranian Hackers Successfully Peddle Stolen Trump Emails," *Reuters*, October 25, 2024. (https://www.reuters.com/world/us/accused-iranian-hackers-successfully-peddle-stolen-trump-emails-2024-10-25)
65. Ibid.
66. "Disrupting a Covert Iranian Influence Operation," *OpenAI*, August 16, 2024. (https://openai.com/index/disrupting-a-covert-iranian-influence-operation); "Influence and Cyber Operations: An Update," *OpenAI*, October 2024. (https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf)
67. Max Lesser and Ari Ben Am, "FDD Identifies 19 Websites as Part of an Iranian Global Influence Operation," *Foundation for Defense of Democracies*, September 6, 2024. (https://www.fdd.org/analysis/2024/09/05/fdd-identifies-19-websites-as-part-of-an-iranian-global-influence-operation); "Iranian IO Domains – Sneak Peak," *Memetic Warfare*, September 6, 2024. (https://www.memeticwarfare.io/p/iranian-io-domains-sneak-peek)
68. Max Lesser and RADM (Ret.) Mark Montgomery, "How U.S. Adversaries Undermine the Perception of Election Integrity," *Foundation for Defense of Democracies*, September 26, 2024. (https://www.fdd.org/wp-content/uploads/2024/09/fdd-memo-how-u.s.-adversaries-undermine-the-perception-of-election-integrity.pdf); Max Lesser, "Foreign Malign Election Meddling Persists But Struggles to Gain Traction," *Foundation for Defense of Democracies*, October 29, 2024. (https://www.fdd.org/wp-content/uploads/2024/10/fdd-memo-foreign-malign-election-meddling-persists-but-struggles-to-gain-traction.pdf)
69. "Russia, Iran, and China Continue Influence Campaigns in Final Weeks Before Election Day 2024," *Microsoft Threat Analysis Center*, October 23, 2024. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-5-on-Russian-Influence.pdf)

in front of the Israeli Embassy in Washington, DC, in February 2024.[70] Bushnell's Men initially encouraged anti-Israel protests across U.S. and European university campuses throughout May 2024. After a four-month hiatus, the campaign resumed in October, focusing on the U.S. elections.[71]

Iranian operatives posed as Americans on X and Telegram and called on U.S. voters to abstain from voting due to Israel's military operation in Gaza.[72] Bushnell's Men also claims to have conducted cyber-enabled influence operations, compromising and defacing websites with the message, "NO CEASEFIRE, NO VOTES." In a Telegram post on October 19, 2024, Bushnell's Men claimed to have hacked over 1,000 American websites.[73] FDD has been unable to corroborate this claim, and archived versions of the domains that Bushnell's Men claims to have hacked show no indication of compromise. It is possible that Bushnell's Men did compromise the websites and the defacements simply were not archived; it is also possible that this represents an attempt at "perception hacking," in which threat actors fabricate or overstate the impact of their operations.

International Union of Virtual Media

The International Union of Virtual Media (IUVM) is an ongoing Iranian influence operation that operates through two domains, iuvmarchive[.]org and iuvmpress[.]co.[74] Researchers have exposed the operation on multiple occasions, yet it persists

Figure: Telegram post from Bushnell's Men cataloging various websites it allegedly hacked and defaced with messages calling for Americans not to vote without a ceasefire between Israel and Hamas

70. "Russia, Iran, and China Continue Influence Campaigns in Final Weeks Before Election Day 2024," *Microsoft Threat Analysis Center*, October 23, 2024. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-5-on-Russian-Influence.pdf); Seth J. Frantzman, "How Is Iran Exploiting the Self-Immolation of U.S. Airman Aaron Bushnell?" *The Jerusalem Post* (Israel), February 27, 2024. (https://www.jpost.com/middle-east/iran-news/article-789129)
71. "Russia, Iran, and China Continue Influence Campaigns in Final Weeks Before Election Day 2024," *Microsoft Threat Analysis Center*, October 23, 2024. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-5-on-Russian-Influence.pdf)
72. Ibid.
73. "Bushnell's Men," *Telegram*, accessed December 5, 2024. (https://ghostarchive.org/archive/wPgtp)
74. Max Lesser, "Foreign Malign Election Meddling Persists But Struggles to Gain Traction," *Foundation for Defense of Democracies*, October 29, 2024. (https://www.fdd.org/wp-content/uploads/2024/10/fdd-memo-foreign-malign-election-meddling-persists-but-struggles-to-gain-traction.pdf)

online.[75] In the month leading up to Election Day, IUVM posted 25 articles about the U.S. elections. While most articles maintained an impartial tone, several criticized Trump, particularly for his rhetoric on immigration, while others called attention to the importance of Arab and Muslim Americans in the U.S. elections.[76] One article also lambasted Trump's October 5, 2024, campaign rally in Butler, PA, writing that Western leaders "are depending more and more on political polarisation, fear-mongering, and conspiracy theories to stay in charge."

Emennet Pasargad

Emennet Pasargad, also known as Cotton Sandstorm and Aria Sepehr Ayandehsazan, is affiliated with the IRGC and has historically distinguished itself as one of the most aggressive Iranian influence operation threat actors.[77] The U.S. government has blamed Emennet Pasargad for two Iranian influence operations targeting the 2020 U.S. presidential election: one in which spoofed emails impersonating the Proud Boys emailed American voters and another that doxxed U.S. election officials.[78] Emennet Pasargad has since carried out multiple operations targeting the United States, Israel, and other countries. Microsoft reported that it observed Emennet Pasargad probing and reconnoitering election-related websites in several U.S. swing states in April 2024 as well as reconnoitering major U.S. media outlets in May 2024, possibly in preparation for an election-related attack. Nevertheless, there is no public reporting that Emennet Pasargad conducted successful cyber or influence operations targeting the 2024 U.S. elections.[79]

75. Jack Stubbs and Christopher Bing, "Exclusive: Iran-Based Political Influence Operation - Bigger, Persistent, Global," *Reuters*, August 28, 2018. (https://www.reuters.com/article/us-usa-iran-facebook-exclusive/exclusive-iran-based-political-influence-operation-bigger-persistent-global-idUSKCN1LD2R9); Max Lesser and RADM (Ret.) Mark Montgomery, "How U.S. Adversaries Undermine the Perception of Election Integrity," *Foundation for Defense of Democracies*, September 26, 2024. (https://www.fdd.org/analysis/2024/09/26/how-u-s-adversaries-undermine-the-perception-of-election-integrity)

76. "The Dangerous Rhetoric of 'Bad Genes': Trump's Controversial Immigration Remarks," *IUVM Archive*, October 8, 2024. (https://web.archive.org/web/20241127005343/https://iuvmpress.co/the-dangerous-rhetoric-of-bad-genes-trumps-controversial-immigration-remarks); "'I'm Not a Nazi,' Trump Asserts as Harris Criticizes 'Ugly Rhetoric' in Close U.S. Election," *IUVM Archive*, October 29, 2024. (https://web.archive.org/web/20241127003410/https://iuvmpress.co/im-not-a-nazi-trump-asserts-as-harris-criticizes-ugly-rhetoric-in-close-us-election); "Trump's MSG Rally Draws Criticism Over Racist Insults and Antagonistic Rhetoric," *IUVM Archive*, October 28, 2024. (https://web.archive.org/web/20241127003719/https://iuvmpress.co/trumps-msg-rally-draws-criticism-over-racist-insults-and-antagonistic-rhetoric); "Arab Americans Take Front Stage in Crucial 2024 Election," *IUVM Archive*, November 5, 2024. (https://web.archive.org/web/20241127002431/https://iuvmpress.co/arab-americans-take-front-stage-in-crucial-2024-election); "Survey Shows 87% of Arab Americans Intend to Vote in U.S. Election, Highlighting Key Swing State Influence," *IUVM Archive*, October 22, 2024. (https://web.archive.org/web/20241127004002/https://iuvmpress.co/survey-shows-87-of-arab-americans-intend-to-vote-in-us-election-highlighting-key-swing-state-influence); "Political Scene Is Heating as the 2024 U.S. Election Gets Ready," *IUVM Archive*, October 18, 2024. (https://web.archive.org/web/20241127004723/https://iuvmpress.co/political-scene-is-heating-as-the-2024-us-election-gets-ready)

77. U.S. Federal Bureau of Investigation, U.S. Department of the Treasury, and Israel National Cyber Directorate, "New Tradecraft of Iranian Cyber Group Aria Sepehr Ayandehsazan aka Emennet Pasargad," October 30, 2024. (https://www.ic3.gov/CSA/2024/241030.pdf)

78. U.S. Department of Justice, Office of Public Affairs, Press Release, "Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election," November 18, 2021. (https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed)

79. "Russia, Iran, and China Continue Influence Campaigns in Final Weeks Before Election Day 2024," *Microsoft Threat Analysis Center*, October 23, 2024. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-5-on-Russian-Influence.pdf)

Hezbollah-Linked Hoopoe Platform

Hoopoe Platform is a pro-Hezbollah, anti-America, and anti-Israel Iranian influence operation first exposed by Recorded Future in August 2024 and further analyzed by FDD in September.[80] Hoopoe Platform operates across various social media platforms, including X, Facebook, Instagram, TikTok, Telegram, LinkedIn, and YouTube. It has proved resilient: while YouTube suspended its account and X suspended two past accounts, Hoopoe Platform now operates a third X account.[81]

Hoopoe Platform has posted content variously supporting and attacking Republican and Democratic presidential candidates, but its main objective appears to be exacerbating political polarization in the United States and undermining faith in democratic institutions.[82] Hoopoe Platform posted content suggesting that American democracy is subverted by Israeli and Jewish financial interests.[83] Other content insinuated that the "deep state" was responsible for the July 2024 assassination attempt against Trump or that a civil war would erupt if Trump lost the election.[84] Some content explicitly called on Americans not to vote for either candidate because "[b]oth are evil and support genocide in Gaza." Other content expressed a desire for third-party candidates to challenge Harris and Trump.[85]

China

China primarily targeted the 2024 U.S. elections through low-quality social media activity. Unlike Russia and Iran, China did not appear to favor Trump or Harris but attacked both major presidential candidates as well as Biden before he dropped out of the race. China did, however, specifically target House and Senate races[86] as Beijing did during the 2022 midterm elections.[87]

80. Insikt Group, "Malign Influence Threats Mount Ahead of U.S. 2024 Elections," *Recorded Future*, August 13, 2024. (https://go.recordedfuture.com/hubfs/reports/ta-2024-0813.pdf); Max Lesser and RADM (Ret.) Mark Montgomery, "How U.S. Adversaries Undermine the Perception of Election Integrity," *Foundation for Defense of Democracies*, September 26, 2024. (https://www.fdd.org/wp-content/uploads/2024/09/fdd-memo-how-u.s.-adversaries-undermine-the-perception-of-election-integrity.pdf)

81. "Iran-Backed 'Hoopoe Platform' Evades Ban Suspension on X, Targets Key 2024 Election Issues Across Four Social Media Platforms," *Alethea*, October 29, 2024. (https://alethea.com/insights/iran-backed-hoopoe-platform-evades-ban-suspension-on-x-targets-key-2024-election-issues-across-four-social-media-platforms)

82. Max Lesser and RADM (Ret.) Mark Montgomery, "How U.S. Adversaries Undermine the Perception of Election Integrity," *Foundation for Defense of Democracies*, September 26, 2024. (https://www.fdd.org/wp-content/uploads/2024/09/fdd-memo-how-u.s.-adversaries-undermine-the-perception-of-election-integrity.pdf)

83. @Hoopoeplatform1, *X*, June 18, 2024. (https://ghostarchive.org/archive/RP7IN); @hoopoeplatform1, *TikTok*, July 30, 2024. (https://ghostarchive.org/archive/D02cr); @Hoopoeplatform1, *X*, July 19, 2024. (https://ghostarchive.org/archive/Mr4QX); @hoopoeplatform1, *TikTok*, July 24, 2024. (https://ghostarchive.org/archive/BITsv)

84. @hoopoeplatform1, *TikTok*, July 24, 2024. (https://ghostarchive.org/archive/7tzCY); @hoopoeplatform1, *TikTok*, July 16, 2024. (https://ghostarchive.org/archive/eElr1); @hoopoeplatform1, *TikTok*, July 17, 2024. (https://ghostarchive.org/archive/Y0cf5); @Hoopoeplatform1, *X*, July 25, 2024. (https://ghostarchive.org/archive/Jsrbo); @Hoopoeplatform1, *X*, July 12, 2024. (https://ghostarchive.org/archive/nS9Tz); @Hoopoeplatform1, *X*, July 24, 2024. (https://ghostarchive.org/archive/EF1vP); Hoopoe Platform, *Facebook*, October 9, 2024. (https://ghostarchive.org/archive/IO9du); Hoopoe Platform, *Facebook*, October 12, 2024. (https://ghostarchive.org/archive/OOStl)

85. Hoopoe Platform, *Facebook*, November 6, 2024. (https://ghostarchive.org/archive/eHo77); Hoopoe Platform, *Facebook*, September 6, 2024. (https://ghostarchive.org/archive/EChcf)

86. Steven Lee Myers, "Bots Linked to China Target Republican House and Senate Candidates, Microsoft Says," *The New York Times*, October 23, 2024. (https://www.nytimes.com/2024/10/23/us/politics/x-bots-china-republicans.html); Christopher Bing and A.J. Vicens, "Chinese Influence Operation Targets U.S. Down-Ballot Races, Microsoft Says," *Reuters*, October 24, 2024. (https://www.reuters.com/world/us/chinese-influence-operation-targets-us-down-ballot-races-microsoft-says-2024-10-23)

87. U.S. Office of the Director of National Intelligence, "Foreign Threats to the 2022 U.S. Elections," December 23, 2022. (https://www.odni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf)

While China's operations targeting down-ballot candidates demonstrate clear attempts to shape voter preferences, Beijing more often spreads content geared toward undermining Americans' faith in their democratic process. China often threads this criticism of American democracy into its broader narrative that the United States is hopelessly dysfunctional and in a state of decline.

Spamouflage

China mostly targeted the election through its flagship online influence operation, Spamouflage. According to Rolling Stone reporter Adam Rawnsley, Spamouflage is run by China's Ministry of Public Security.[88] Spamouflage, also known as Dragonbridge, Empire Dragon, Taizi Flood, and Storm-1376, began targeting American audiences in 2020 and typically produces a high volume of low-quality content across major social media platforms. This content usually garners very limited authentic engagement.

In February 2024, the Institute for Strategic Dialogue (ISD) first reported on Spamouflage's operations targeting the 2024 U.S. elections, noting that Spamouflage's X posts date back to at least October 2023.[89] This timeline aligns with separate FDD research on Spamouflage's activity on Facebook.[90] ISD observed Spamouflage posing as Trump supporters to push pro-Trump content and using generative AI to create political cartoons.[91] FDD also found evidence of Spamouflage using automation to generate text in its comments on Facebook.[92]

Spamouflage criticized all major presidential candidates without showing a clear preference.[93] Spamouflage often criticized presidential candidates for their support for Israel, contending that Israel controls all American candidates.[94]

Spamouflage did, however, attempt to undermine specific candidates in several congressional races. It targeted Republicans critical of China, including Senator Marco Rubio of Florida, Representative Barry Moore of Alabama, Representative Michael McCaul of Texas, Senator Marsha Blackburn of Tennessee, and Representative Young Kim of

88. Adam Rawnsley, "Chinese Intel Officers Interfered in U.S. Election," *The Rolling Stone*, August 29, 2023. (https://www.rollingstone.com/politics/politics-features/china-facebook-instagram-propaganda-campaign-1234813762)
89. Elise Thomas, "Pro-CCP 'Spamouflage' Network Pivoting to Focus on U.S. Presidential Election," *Institute for Strategic Dialogue*, February 15, 2024. (https://www.isdglobal.org/digital_dispatches/pro-ccp-spamouflage-net-work-focuses-on-us-election)
90. Max Lesser, Ari Ben Am, Margot Fulde-Hardy, Saman Nazari, and Paul J. Malcomb, "Much Ado About 'Somethings': China-Linked Influence Operation Endures Despite Takedowns," *Foundation for Defense of Democracies*, March 27, 2024. (https://www.fdd.org/analysis/2024/03/27/much-ado-about-somethings)
91. Elise Thomas, "Pro-CCP Spamouflage Campaign Experiments with New Tactics Targeting the U.S.," *Institute for Strategic Dialogue*, April 1, 2024. (https://www.isdglobal.org/digital_dispatches/pro-ccp-spamouflage-campaign-experiments-with-new-tactics-targeting-the-us)
92. Max Lesser, Ari Ben Am, Margot Fulde-Hardy, Saman Nazari, and Paul J. Malcomb, "Much Ado About 'Somethings': China-Linked Influence Operation Endures Despite Takedowns," *Foundation for Defense of Democracies*, March 27, 2024. (https://www.fdd.org/analysis/2024/03/27/much-ado-about-somethings)
93. Elise Thomas, "Pro-CCP 'Spamouflage' Network Pivoting to Focus on U.S. Presidential Election," *Institute for Strategic Dialogue*, February 15, 2024. (https://www.isdglobal.org/digital_dispatches/pro-ccp-spamouflage-net-work-focuses-on-us-election); Max Lesser, Ari Ben Am, Margot Fulde-Hardy, Saman Nazari, and Paul J. Malcomb, "Much Ado About 'Somethings': China-Linked Influence Operation Endures Despite Takedowns," *Foundation for Defense of Democracies*, March 27, 2024. (https://www.fdd.org/analysis/2024/03/27/much-ado-about-somethings); Max Lesser, "Foreign Malign Election Meddling Persists But Struggles to Gain Traction," *Foundation for Defense of Democracies*, October 29, 2024. (https://www.fdd.org/analysis/2024/10/29/foreign-malign-election-meddling-persists-but-struggles-to-gain-traction)
94. "Inauthentic Chinese X Accounts Amplifying Trump Shooting and Biden Withdrawal Conspiracy Theories," *Digital Forensic Research Lab*, July 30, 2024. (https://dfrlab.org/2024/07/30/china-x-trump-biden-harris)

California.[95] Spamouflage's attacks on Moore notably criticized his support for Israel and resorted to antisemitic language, aligning with a larger trend in which Spamouflage has leveraged antisemitism to promote anti-Western narratives.[96]

Microsoft also observed a Chinese operation it calls Storm-1852 posing as Trump supporters. The operation created short-form video content, reposted other content, and organized "follow trains."[97] While Microsoft refers to this campaign as separate from Spamouflage, Microsoft's analysis pertains to the same cluster of X accounts that many other researchers have referred to as Spamouflage. Microsoft notes that some accounts associated with Storm-1852 posted content that received hundreds of thousands of views, distinguishing it as some of the most successful Chinese influence operation activity targeting the 2024 U.S. elections.[98]

Post-Election Content

Since the election, FDD has observed several notable findings relating to foreign influence operations. Russia's Portal Kombat continued to post anti-Harris content while also sharing several articles questioning the outcome of the election. News-pravda[.]com, for example, republished an article from Russian state-media outlet RIAN that suggests that some electors might choose not to cast their electoral college ballots for Trump, instead voting for Harris and handing her the presidency.[99] Another news-pravda[.]com article republished content from British tabloid The Daily Mail depicting a hypothetical scenario in which Biden would resign so that Harris could assume the presidency and brand Trump as a terrorist.[100]

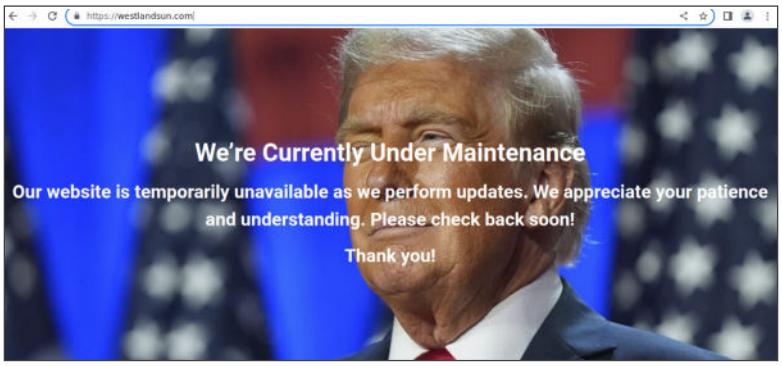

Figure: The landing page for westlandsun[.]com as of November 27, 2024, after having gone offline for several weeks.

95. Christopher Bing and A.J. Vicens, "Chinese Influence Operation Targets U.S. Down-Ballot Races, Microsoft Says," *Reuters*, October 24, 2024. (https://www.reuters.com/world/us/chinese-influence-operation-targets-us-down-ballot-races-microsoft-says-2024-10-23)
96. "Russia, Iran, and China Continue Influence Campaigns in Final Weeks Before Election Day 2024," *Microsoft Threat Analysis Center*, October 23, 2024. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC-Report-Russia-Iran-and-China-continue-influence-campaigns-in-final-weeks-October-23-2024.pdf); Wenhao Ma, "China-Connected Spamouflage Networks Spread Antisemitic Disinformation," *Voice of America*, October 4, 2024. (https://www.voanews.com/a/china-connected-spamouflage-networks-spread-antisemitic-disinformation/7811033.html)
97. "Russia Leverages Cyber proxies and Volga Flood Assets in Expansive Influence Efforts," *Microsoft Threat Analysis Center*, September 17, 2024. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-4.pdf)
98. "Iran Steps Into U.S. Election 2024 With Cyber-Enabled Influence Operations," *Microsoft Threat Analysis Center*, August 9, 2024, page 7. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf)
99. "Trump May Still Lose: Democrats Have a Decisive Trump Card in Store," *News Pravda*, November 6, 2024. (https://web.archive.org/web/20241120185754/https://news-pravda.com/world/2024/11/06/830682.html)
100. "After the U.S. Elections, a War Will Begin: Britain Published a Scenario of Riots After the Victory of Trump or Harris," *News Pravda*, November 6, 2024. (https://web.archive.org/web/20241120184427/https://news-pravda.com/usa/2024/11/06/832034.html)

Regarding Iranian operations, by November 7, savannahtime[.]com, westlandsun[.]com, niothinker[.]com, and afromajority[.]com were no longer online.[101] This suggests either that their Iranian operatives dismantled the websites after they served their election-related purposes or that law enforcement or the hosting provider took down the sites.

The landing page for afromajority[.]com now features a notice that the domain's registrant account has been suspended, indicating that the registrar took action against the domain for violating the terms of service.[102] Westlandsun[.]com, after a brief hiatus, is once again online, although the landing page includes a notice stating that the website is undergoing maintenance. Curiously, the landing page features a background image depicting Trump winking, an unusual choice given that the domain had previously criticized him. This image choice could suggest a potential future shift in the domain's political orientation or simply an effort to troll Americans.[103]

Since the election, teorator[.]com has continued to publish content, mainly criticizing Harris's campaign strategy as being divisive while also celebrating Trump's victory as heralding the end of the "deep state."[104] Evenpolitics[.]com has also published post-election content. Several articles decry Trump's cabinet nominations and make light of his electoral victory, though other articles criticize the Democratic Party and American media.[105] Curiously,

101. Savannahtime[.]com, accessed November 7, 2024. (https://ghostarchive.org/archive/RsT4b); westlandsun[.]com, accessed November 7, 2024. (https://ghostarchive.org/archive/9efDa); niothinker[.]com, accessed November 7, 2024. (https://ghostarchive.org/archive/QG1n8); afromajority[.]com accessed November 7, 2024. (https://ghostarchive.org/archive/rhqos)

102. Afromajority[.]com, accessed November 27, 2024. (https://web.archive.org/web/20241127220046/https://afromajority.com/cgi-sys/suspendedpage.cgi); "Afromajority[.]com," *VirusTotal*, accessed November 27, 2024. (https://www.virustotal.com/gui/domain/afromajority.com/associations)

103. Westlandsun[.]com, accessed November 27, 2024. (https://web.archive.org/web/20241127215655/https://westlandsun.com)

104. "John Ratcliffe's Mission: Reforming the CIA and Confronting the Deep State," *Teorator*, November 20, 2024. (https://web.archive.org/web/20241127214341/https://teorator.com/index.php/2024/11/20/john-ratcliffes-mission-reforming-the-cia-and-confronting-the-deep-state); "Leftist Meltdown: The Hypocrisy Behind the "Tolerant" Crowd's Post-Election Tantrum," *Teorator*, November 23, 2024. (https://web.archive.org/web/20241127214126/https://teorator.com/index.php/2024/11/23/leftist-meltdown-the-hypocrisy-behind-the-tolerant-crowds-post-election-tantrum); "The Awakening of America: A Call for Renewal," *Teorator*, November 22, 2024. (https://web.archive.org/web/20241127214144/https://teorator.com/index.php/2024/11/22/the-awakening-of-america-a-call-for-renewal); "Real Talk: Why the Democratic 'Girl Boss' Narrative Derailed Hillary and Kamala," *Teorator*, November 9, 2024. (https://web.archive.org/web/20241127213903/https://teorator.com/index.php/2024/11/09/real-talk-why-the-democratic-girl-boss-narrative-derailed-hillary-and-kamala); "Kamala's Celebrity Stunt Backfires as Out-of-Touch Elitism Sinks Her Campaign," *Teorator*, November 9, 2024. (https://web.archive.org/web/20241127214344/https://teorator.com/index.php/2024/11/09/kamalas-celebrity-stunt-backfires-as-out-of-touch-elitism-sinks-her-campaign)

105. "Pam Bondi as Trump's Attorney General? Democrats Need to Fight Like Hell," *Even Politics*, November 25, 2024. (https://web.archive.org/web/20241127210223/https://evenpolitics.com/2024/11/25/pam-bondi-as-trumps-attorney-general-democrats-need-to-fight-like-hell); "Trump's Latest Pick Could Unleash a Wave of Dangerous Food Deregulation," *Even Politics*, November 25, 2024. (https://web.archive.org/web/20241127210438/https://evenpolitics.com/2024/11/25/trumps-latest-pick-could-unleash-a-wave-of-dangerous-food-deregulation); "RFK Jr.: A Dangerous Gamble for Public Health?" *Even Politics*, November 24, 2024. (https://web.archive.org/web/20241127210731/https://evenpolitics.com/2024/11/24/rfk-jr-a-dangerous-gamble-for-public-health); "Donald Trump's New FCC Pick: Brendan Carr's Dangerous Agenda," *Even Politics*, November 19, 2024. (https://web.archive.org/web/20241127211236/https://evenpolitics.com/2024/11/19/donald-trumps-new-fcc-pick-brendan-carrs-dangerous-agenda); "Matt Gaetz as Attorney General? Trump's Latest Pick is Short on Experience, Long on Loyalty," *Even Politics*, November 19, 2024. (https://web.archive.org/web/20241127211652/https://evenpolitics.com/2024/11/19/matt-gaetz-as-attorney-general-trumps-latest-pick-is-short-on-experience-long-on-loyalty); "Kamala Harris's Campaign Is Over. So Is the Media's Credibility," *Even Politics*, November 26, 2024. (https://web.archive.org/web/20241127205344/https://evenpolitics.com/2024/11/26/kamala-harriss-campaign-is-over-so-is-the-medias-credibility); "Kamala Harris Spent $1.5 Billion in 15 Weeks — And What Does She Have to Show for It?" *Even Politics*, November 21, 2024. (https://web.archive.org/web/20241127211636/https://evenpolitics.com/2024/11/21/kamala-harris-spent-1-5-billion-in-15-weeks-and-what-does-she-have-to-show-for-it); "Will Rich Liberals Wake Up Before It's Too Late? MSNBC's Spin-Off Is a Warning Sign," *Even Politics*, November 26, 2024. (https://web.archive.org/web/20241127205002/https://evenpolitics.com/2024/11/26/will-rich-liberals-wake-up-before-its-too-late-msnbcs-spin-off-is-a-warning-sign)

contrary to its stance as a progressive media outlet, evenpolitics[.]com has also published several articles viewing Trump somewhat sympathetically.[106]

Artificial Intelligence in Foreign Malign Influence Targeting the 2024 U.S. Elections

In the lead-up to Election Day, researchers and government officials warned that America's adversaries would use AI to improve their influence operations dramatically.[107] While Russia, Iran, and China all used AI-generated content in their influence operations, this did not appear to transform their operations.[108] AI allowed adversaries to create content at scale more easily, but it did not improve the quality of their operations.

China's Spamouflage, for example, used generative AI to create political cartoons, but these cartoons generally appeared to garner little engagement on social media.[109] A Russian operation used AI to clone the FBI director's voice and allege massive voter fraud, but this content was quickly debunked by the media and does not appear to have convinced many American voters to contest the results of the 2024 U.S. elections.[110] An Iranian operation utilized generative AI to create text for its websites targeting American voters, but both FDD and Microsoft found that few people visited these websites.[111]

By contrast, the Russian hoax videos that went viral in the weeks leading up to the election leveraged a well-established tactic of using paid actors.[112] Iran's most high-profile operation, involving the hack and leak of Trump campaign materials, appears to have used a spear-phishing attack rather than a sophisticated AI-enabled cyberattack.

106. "The Squirrel, the Lights, and Why No One's Fixing Anything," *Even Politics*, November 26, 2024. (https://web.archive.org/web/20241127203847/https://evenpolitics.com/2024/11/26/the-squirrel-the-lights-and-why-no-ones-fixing-anything); "The Audacity of Mercy: Why We Should Let Trump Off the Hook (Sort Of)," *Even Politics*, November 25, 2024. (https://web.archive.org/web/20241127205836/https://evenpolitics.com/2024/11/25/the-audacity-of-mercy-why-we-should-let-trump-off-the-hook-sort-of)

107. Devin Dwyer and Sarah Herndon, "AI Deepfakes a Top Concern for Election Officials With Voting Underway," *ABC News*, October 18, 2024. (https://abcnews.go.com/Politics/ai-deepfakes-top-concern-election-officials-voting-underway/story?id=114202574); U.S. Office of the Director of National Intelligence, Press Release, "DNI Haines Opening Statement as Delivered to the SSCI for An Update on Foreign Threats to the 2024 Elections," May 15, 2024. (https://www.dni.gov/index.php/newsroom/congressional-testimonies/congressional-testimonies-2024/3823-dni-haines-opening-statement-as-delivered-to-the-ssci-for-an-update-on-foreign-threats-to-the-2024-elections)

108. U.S. Office of the Director of National Intelligence, "45 Days Until Election 2024: Election Security Update as of Mid-September 2024," September 23, 2024. (https://www.odni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240923.pdf)

109. Elise Thomas, "Pro-CCP 'Spamouflage' Network Pivoting to Focus on U.S. Presidential Election," *Institute for Strategic Dialogue*, February 15, 2024. (https://www.isdglobal.org/digital_dispatches/pro-ccp-spamouflage-net-work-focuses-on-us-election)

110. "Investigation: Chinese Bot Network Is Amplifying Russian Disinformation About the U.S. Election," *Digital Forensic Research Lab*, November 5, 2024. (https://dfrlab.org/2024/11/05/russia-china-us-election-operation-overload); Derek B. Johnson, "FBI Flags False Videos Impersonating Agency, Claiming Democratic Ballot Fraud," *CyberScoop*, November 2, 2024. (https://cyberscoop.com/fbi-fake-videos-ballot-fraud-democrats-doppelganger)

111. "Iran Steps Into U.S. Election 2024 With Cyber-Enabled Influence Operations," *Microsoft Threat Analysis Center*, August 9, 2024. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf)

112. "Russia, Iran, and China Continue Influence Campaigns in Final Weeks Before Election Day 2024," *Microsoft Threat Analysis Center*, October 23, 2024. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-5-on-Russian-Influence.pdf)

A statement from the U.S. Office of the Director of National Intelligence (ODNI) in mid-September best sums up the impact of AI on foreign malign influence targeting the 2024 U.S. elections. ODNI noted that generative AI helped "improve and accelerate aspects of foreign influence operations," but it did not "revolutionize such operations."[113]

Still, the threat should not be dismissed entirely. AI-generated deepfakes have arguably played a significant role in foreign elections, most notably in Slovakia in 2023. The capability to rapidly identify and verify AI-generated content will remain important in future U.S. elections.[114]

U.S. Government Response

The collective efforts of the U.S. government, private sector, non-profits, and academia helped expose and thwart foreign malign influence campaigns targeting American voters. The earlier sections of this report repeatedly reference research by private companies and non-profits, demonstrating the breadth and depth of information from organizations across these sectors. At the same time, the U.S. government proved particularly effective and efficient this election cycle. It debunked falsehoods in near-real time, preemptively warned Americans of adversaries' TTPs, took down infrastructure enabling influence operations, and name-and-shamed malign influence actors.

U.S. government organizations involved in combating foreign malign influence targeting the 2024 U.S. elections included ODNI's Foreign Malign Influence Center, the FBI's Foreign Influence Task Force, CISA, DOJ, the State Department, and the Treasury Department. Interagency coordination was evident. Occasionally, the U.S. government also partnered with America's democratic allies in combating foreign malign influence. For example, the FBI, Treasury, and Israel's National Cyber Directorate released a joint cybersecurity advisory on Emennet Pasargad.[115]

In April 2024, the U.S. government released what appears to be its earliest public statement on foreign malign influence targeting the 2024 elections. CISA, the FBI, and ODNI put out a helpful overview that defined foreign malign influence, specified which of America's adversaries were most likely to target U.S. elections, and detailed the TTPs these adversaries might employ.[116] Many of the TTPs outlined in this document, from voice cloning to cyber-enabled influence operations, actually occurred during the 2024 election cycle.

ODNI's Foreign Malign Influence Center continued to release regular updates from May through the end of October.[117] In addition, CISA, the FBI, and ODNI continued to collaborate to provide information to the public

113. U.S. Office of the Director of National Intelligence, "45 Days Until Election 2024: Election Security Update as of Mid-September 2024," September 23, 2024. (https://www.odni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240923.pdf)
114. U.S. Office of the Director of National Intelligence, Press Release, "DNI Haines Opening Statement as Delivered to the SSCI for An Update on Foreign Threats to the 2024 Elections," May 15, 2024. (https://www.dni.gov/index.php/newsroom/congressional-testimonies/congressional-testimonies-2024/3823-dni-haines-opening-statement-as-delivered-to-the-ssci-for-an-update-on-foreign-threats-to-the-2024-elections)
115. U.S. Federal Bureau of Investigation, U.S. Department of the Treasury, and Israel National Cyber Directorate, "New Tradecraft of Iranian Cyber Group Aria Sepehr Ayandehsazan aka Emennet Pasargad," October 30, 2024. (https://www.ic3.gov/CSA/2024/241030.pdf)
116. U.S. Cybersecurity and Infrastructure Security Agency, U.S. Federal Bureau of Investigation, and U.S. Office of the Director of National Intelligence, "Securing Election Infrastructure Against the Tactics of Foreign Malign Influence Operations," April 2024. (https://www.cisa.gov/sites/default/files/2024-04/Securing_Election_Infrastructure_Against_the_Tactics_of_Foreign_Malign_Influence_Operations_2024FINAL_508c.pdf)
117. "Newsroom," . U.S. *Office of the Director of National Intelligence, The Foreign Malign Influence Center*, accessed December 5, 2024. (https://www.dni.gov/index.php/fmic-news)

regarding foreign malign influence, including on specific incidents such as the hoax videos spread by CopyCop.[118] Often, these official statements debunked the malign content within days of it going viral.

The efforts of state and local governments were also critical. The office of the Georgia secretary of state, the Bucks County Board of Elections, and the San Francisco Police Department, for example, all issued statements either directly to the public or to the media debunking videos likely originating from CopyCop.[119]

Meanwhile, the U.S. government exposed and dismantled Russian and Iranian influence networks. In March 2024, Treasury sanctioned two individuals behind Doppelganger.[120] In early September, DOJ indicted Russian individuals who conspired to fund an unnamed Tennessee-based digital media company to push Kremlin-aligned content.[121] That same day, the department announced the seizure of 32 domains associated with Doppelganger,[122] and Treasury sanctioned 10 individuals connected with Russian malign influence targeting the 2024 elections.[123] Later that month, DOJ unsealed an indictment against three members of the IRGC for its hack-and-leak operations targeting the Trump campaign,[124] while Treasury sanctioned seven individuals associated with Iranian state-sponsored cyber-enabled influence operations targeting U.S. elections.[125]

The U.S. government did a good job of getting out ahead of potential election integrity concerns and threats. CISA and the FBI proactively issued joint statements reassuring citizens that cyberattacks would not interfere with their

118. U.S. Cybersecurity and Infrastructure Security Agency, Press Release, "Joint ODNI, FBI, and CISA Statement," November 4, 2024. (https://www.cisa.gov/news-events/news/joint-odni-fbi-and-cisa-statement-1); U.S. Cybersecurity and Infrastructure Security Agency, Press Release, "Joint ODNI, FBI, and CISA Statement on Russian Election Influence Efforts," November 1, 2024. (https://www.cisa.gov/news-events/news/joint-odni-fbi-and-cisa-statement-russian-election-influence-efforts); U.S. Cybersecurity and Infrastructure Security Agency, Press Release, "Joint ODNI, FBI, and CISA Statement," October 25, 2024. (https://www.cisa.gov/news-events/news/joint-odni-fbi-and-cisa-statement-0)

119. Office of Georgia Secretary of State, "Statement from Secretary Raffensperger," October 31, 2024. (https://sos.ga.gov/news/statement-secretary-raffensperger); "Board of Elections Issues Bipartisan Statement on Fake Ballot Video," *Bucks County, Pennsylvania*, October 24, 2024. (https://www.buckscounty.gov/CivicAlerts.aspx?AID=1151); "Fact Check: Video of Pennsylvania Mail-in Ballots Being Destroyed Is Fake," *Reuters*, October 31, 2024. (https://www.reuters.com/fact-check/video-pennsylvania-mail-in-ballots-being-destroyed-is-fake-2024-10-31); "Fact Check: Kamala Harris Hit-and-Run Story Stems From Unreliable Website," *Reuters*, September 20, 2024. (https://www.reuters.com/fact-check/kamala-harris-hit-and-run-story-stems-unreliable-website-2024-09-20)

120. U.S. Department of the Treasury, Press Release, "Treasury Sanctions Actors Supporting Kremlin-Directed Malign Influence Efforts," March 20, 2024. (https://home.treasury.gov/news/press-releases/jy2195)

121. U.S. Department of Justice, Office of Public Affairs, Press Release, "Two RT Employees Indicted for Covertly Funding and Directing U.S. Company that Published Thousands of Videos in Furtherance of Russian Interests," September 4, 2024. (https://www.justice.gov/opa/pr/two-rt-employees-indicted-covertly-funding-and-directing-us-company-published-thousands); Andrew Couts and Tim Marchman, "Right-Wing Influencer Network Tenet Media Allegedly Spread Russian Disinformation," *Wired*, September 4, 2024. (https://www.wired.com/story/right-wing-influencer-network-tenet-media-allegedly-spread-russian-disinformation)

122. U.S. Department of Justice, Office of Public Affairs, Press Release, "Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere," September 4, 2024. (https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence)

123. U.S. Department of the Treasury, Press Release, "Treasury Takes Action as Part of a U.S. Government Response to Russia's Foreign Malign Influence Operations," September 4, 2024. (https://home.treasury.gov/news/press-releases/jy2559)

124. U.S. Department of Justice, Office of Public Affairs, Press Release, "Three IRGC Cyber Actors Indicted for 'Hack-and-Leak' Operation Designed to Influence the 2024 U.S. Presidential Election," September 27, 2024. (https://www.justice.gov/opa/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us)

125. U.S. Department of the Treasury, Press Release, "Treasury Sanctions Iranian Regime Agents Attempting to Interfere in U.S. Elections," September 27, 2024. (https://home.treasury.gov/news/press-releases/jy2621)

ability to vote.[126] CISA and the FBI also warned that adversaries might falsely claim to have hacked voting machines to undermine public faith in election integrity.[127] In addition, CISA and the U.S. Election Assistance Commission published an incident response communication guide to provide election officials with best practices for communicating cyber incidents to relevant officials, the media, and the public should something more significant occur.[128]

Moreover, CISA and the FBI provided specific guidance meant to protect political organizations against Iranian cyberattacks, including instructions for senior government officials, think tank personnel, journalists, activists, and lobbyists on how to harden their systems.[129] Less than three weeks before Election Day, CISA and the FBI issued a public statement detailing various activities by Russian and Iranian threat actors.[130] Importantly, ODNI warned in October that foreign malign influence targeting the 2024 U.S. elections might not stop when voting ends, outlining how adversaries could try to sow chaos and division between Election Day and the presidential inauguration.[131]

On Election Day, the FBI responded quickly to the hoax bomb threats, assuring the public that none of the threats were credible.[132] CISA, for its part, released a statement the next day affirming the security and integrity of election infrastructure.[133]

Recommendations

America proved remarkably more resilient to foreign malign influence in 2024 compared to previous election cycles. This success does not mean that foreign malign influence does not present a significant threat, however. American society must remain vigilant lest the nation regress to its earlier state of vulnerability.

126. U.S. Federal Bureau of Investigation and U.S. Cybersecurity and Infrastructure Security Agency, "Just So You Know: DDoS Attacks Could Hinder Access to Election Information, Would Not Prevent Voting," July 31, 2024. (https://www.cisa.gov/sites/default/files/2024-07/DDoS-FBI-CISA-PSA-508c.pdf); U.S. Federal Bureau of Investigation and U.S. Cybersecurity and Infrastructure Security Agency, "Just So You Know: Ransomware Disruptions During Voting Periods Will Not Impact the Security and Resilience of Vote Casting or Counting," August 15, 2024. (https://www.cisa.gov/sites/default/files/2024-08/Just_So_You_Know_Ransomware_Disruptions_During_Voting_Periods_Will_Not_Impact_the_Security_and_Resilience_of_Vote_Casting_or_Counting_8.15.24_V2_508c_0.pdf)

127. U.S. Cybersecurity and Infrastructure Security Agency and U.S. Federal Bureau of Investigation, "Just So You Know: False Claims of Hacked Voter Information Likely Intended to Sow Distrust of U.S. Elections," September 12, 2024. (https://www.cisa.gov/sites/default/files/2024-09/PSA_Just_So_You_Know_False_Claims_of_Hacking_Voter_Reg_CISA_and_FBI-508_0.pdf)

128. U.S. Cybersecurity and Infrastructure Security Agency and U.S. Election Assistance Commission, "Election Infrastructure Incident Response Communications Guide," October 2024. (https://www.cisa.gov/sites/default/files/2024-10/Election-Infrastructure-Incident-Response-Communications-Guide-508.pdf)

129. U.S. Cybersecurity and Infrastructure Security Agency and U.S. Federal Bureau of Investigation, "How to Protect against Iranian Targeting of Accounts Associated with National Political Organizations," October 2024. (https://www.cisa.gov/sites/default/files/2024-10/cisa-fbi-protecting-against-irgc-phishing-508c.pdf)

130. U.S. Federal Bureau of Investigation and U.S. Cybersecurity and Infrastructure Security Agency, "Just So You Know: Foreign Threat Actors Likely to Use a Variety of Tactics to Develop and Spread Disinformation During 2024 U.S. General Election Cycle," October 18, 2024. (https://www.cisa.gov/sites/default/files/2024-10/PSA_Just_So_You_Know_Foreign_Threat_Actors_Likely_to_Use_a_Variety_of_TacticsV2-508.pdf)

131. U.S. Office of the Director of National Intelligence, National Intelligence Council, "Foreign Threats to U.S. Elections After Voting Ends in 2024," October 8, 2024. (https://www.dni.gov/files/ODNI/documents/assessments/NICM-Declassified-Foreign-Threats-to-US-Elections-After-Voting-Ends-in-2024.pdf)

132. U.S. Federal Bureau of Investigation, National Press Office, Press Release, "FBI Statement on Bomb Threats to Polling Locations," November 5, 2024. (https://www.fbi.gov/news/press-releases/fbi-statement-on-bomb-threats-to-polling-locations)

133. U.S. Cybersecurity and Infrastructure Security Agency, "Statement from CISA Director Easterly on the Security of the 2024 Elections," November 6, 2024. (https://www.cisa.gov/news-events/news/statement-cisa-director-easterly-security-2024-elections)

The following recommendations are meant for actors across American society, including the U.S. government, private-sector organizations such as major tech platforms, and researchers across the for-profit, non-profit, and academic community.

1. **Distinguish between foreign malign influence and domestic falsehoods:** All parties involved in countering foreign malign influence — whether in the public, private, or non-profit sectors — must always clearly distinguish between foreign malign influence and constitutionally protected speech. Domestic speech, even when patently false or parroting foreign propaganda, constitutes constitutionally protected free speech. The Constitution, however, does not protect foreign, covert efforts to influence American public opinion. The following statement by the State Department provides a model for how to distinguish between covert influence and free expression:

   > "The United States supports the free flow of information. We are not taking action against these entities and individuals for the content of their reporting, or even the disinformation they create and spread publicly. We are taking action against them for their covert influence activities. Covert influence activities are not journalism."[134]

2. **Continue to support interagency efforts to counter foreign malign influence:** The U.S. government must continue to support efforts to counter foreign malign influence across the interagency. Federal agencies proved remarkably effective at informing the public of foreign malign influence and, to a degree, even disrupting these operations. The U.S. government should continue to treat foreign malign influence as a national security issue and ensure that ODNI's Foreign Malign Influence Center, the FBI's Foreign Influence Task Force, and CISA have the proper funding to continue their work. While the State Department's Global Engagement Center focuses on foreign malign influence targeting foreign countries, it also plays a crucial role in defending America and its allies. For example, after Russian disinformation contributed to U.S. troops withdrawing from Niger in March 2024, the head of U.S. Africa Command called for more support from the Global Engagement Center to help prevent events like this in the future.[135]

3. **Clean up social media to proactively remove and prevent the creation of fake accounts:** Chinese operations such as Spamouflage and Russian operations such as Doppelganger have easily reconstituted themselves after being taken down by social media platforms. In part, this is because threat actors can easily acquire fake accounts to resume their influence operations. Social media companies should implement measures to proactively take down and prevent the creation of fake accounts on their platforms. Though mainstream social media companies often take significant actions to remove fake accounts, more can be done.[136] In an October 2024 report, FDD suggested a number of measures that can assist with these efforts, from strengthening identity verification to proactively identifying loopholes that allow users to create fake accounts en masse.[137]

4. **Strengthen know-your-customer processes for hosting services in America and Europe:** America's adversaries strive to acquire access to Western hosting services for the purposes of both cybercrime and malign influence operations. This is because Western hosting services are generally reliable and, more importantly, are less likely to

134. U.S. Department of State, Office of the Spokesperson, Press Release, "Alerting the World to RT's Global Covert Activities," September 13, 2024. (https://www.state.gov/alerting-the-world-to-rts-global-covert-activities)
135. Patrick Tucker, "Russia's lies helped persuade Niger to eject US troops, AFRICOM says," *Defense One*, March 21, 2024. (https://www.defenseone.com/threats/2024/03/top-us-commander-africa-pleads-resources-counter-russian-disinformation/395145)
136. Ernestas Naprys, "Facebook has deleted four planets' worth of fake users – while real people struggle to get support," *Cybernews*, November 15, 2023. (https://cybernews.com/editorial/facebook-deleted-billions-fake-users)
137. Max Lesser, Sophie McDowall, and Cat Smith, "Nip the Bots in the Bud: Proactively Taking Down and Preventing the Creation of Inauthentic Social Media Entities," *Foundation for Defense of Democracies*, October 10, 2024. (https://www.fdd.org/analysis/2024/10/10/nip-the-bots-in-the-bud)

attract scrutiny from governments or users. This leads adversaries to take effort-intensive steps to access Western hosting infrastructure, including setting up front companies.[138] If America and its allies require hosting servers in America and Europe to strengthen their know-your-customer processes — for example, by limiting the amount of infrastructure one can buy without photo ID — then threat actors would have a harder time accessing hosting infrastructure by misrepresenting their identities. Broader efforts to prevent the creation of front companies will also help prevent adversaries from accessing hosting infrastructure. While stronger processes may never fully mitigate the cyber and malign influence threats, they can make these operations more costly and difficult.

5. **Integrate practices from cyber threat intelligence into foreign malign influence research:** Cyber threat intelligence reports regularly publish technical indicators, such as phishing email patterns and IP addresses. The community of researchers focused on foreign malign influence should similarly share technical indicators in their reports. Some companies have started to do this, but it should become the norm across the public, private, and non-profit sectors. This information would help analysts build off each other's work. It would also help threat intelligence companies and others create tools that can detect patterns indicative of malicious behavior.
6. **Deter malicious behavior from adversaries:** Taking down domains and accounts supporting influence operations is great, but adversaries will quickly adapt and resume their operations, as the cases of Doppelganger and Spamouflage demonstrate.[139] Deterring adversaries from conducting these operations in the first place would be more efficient and effective. To deter malicious behavior, the U.S. government should impose more significant costs on threat actors and the nation-states that back them. Washington has previously imposed sanctions against individuals involved in malign influence operations. The government should study the effectiveness of these sanctions in deterring malign influence and consider other measures if the sanctions are found to be ineffective.

Conclusion

The United States proved resilient against foreign malign influence targeting the 2024 U.S. elections. Federal, state, and local officials, along with social media companies and researchers, worked proactively to safeguard U.S. election integrity. Adversary operations might have achieved greater impact had this activity gone undetected.

Nevertheless, America must remain vigilant. Foreign malign influence is a national security issue and should not be made into a partisan one. The United States should continue to support and enhance the institutions and communities that combat such influence so that come 2026 and 2028, the country can again celebrate its success in preserving election integrity. These efforts will help preserve America's way of life while demonstrating to adversaries and allies alike that the United States remains strong and resilient.

138. U.S. Federal Bureau of Investigation, U.S. Department of the Treasury, and Israel National Cyber Directorate, "New Tradecraft of Iranian Cyber Group Aria Sepehr Ayandehsazan aka Emennet Pasargad," October 30, 2024. (https://www.ic3.gov/CSA/2024/241030.pdf); Qurium, "How Russia Uses EU Companies for Propaganda," July 11, 2024. (https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation)

139. Esteban Ponce de León, "Doppelganger Websites Persist One Month Following U.S. Government Seizures," *Digital Forensic Research Lab*, October 9, 2024. (https://dfrlab.org/2024/10/09/doppelganger-websites-persist)

Foundation for Defense of Democracies (FDD)

FDD is a Washington, DC-based nonpartisan research institute focusing on national security and foreign policy.

FDD's Center on Cyber and Technology Innovation

FDD's Center on Cyber and Technology Innovation (CCTI) seeks to advance U.S. prosperity and security through technology innovation while countering cyber threats that seek to diminish it. CCTI promotes a greater understanding within the U.S. government, private sector, and allied countries of the threats to and opportunities for national security presented by the rapidly expanding technological environment.

Max Lesser is the senior analyst on emerging threats at FDD's Center on Cyber and Technology Innovation. Max previously served as head of U.S. policy analysis and engagement at Darktrace Federal, where he analyzed policy initiatives surrounding artificial intelligence and cybersecurity.

Mason Krusch is an intern with FDD's Center on Cyber and Technology Innovation and an independent researcher specializing in foreign malign influence operations, anti-government extremism, and cybercrime.

Ari Ben Am is an adjunct fellow at FDD's Center on Cyber and Technology Innovation. His research focuses on emerging threats, influence and information operations, cyber operations, and hybrid warfare. Ari is an open-source intelligence analyst by trade and the co-founder of Telemetry Data Labs, a Telegram data analytics and investigation platform.
