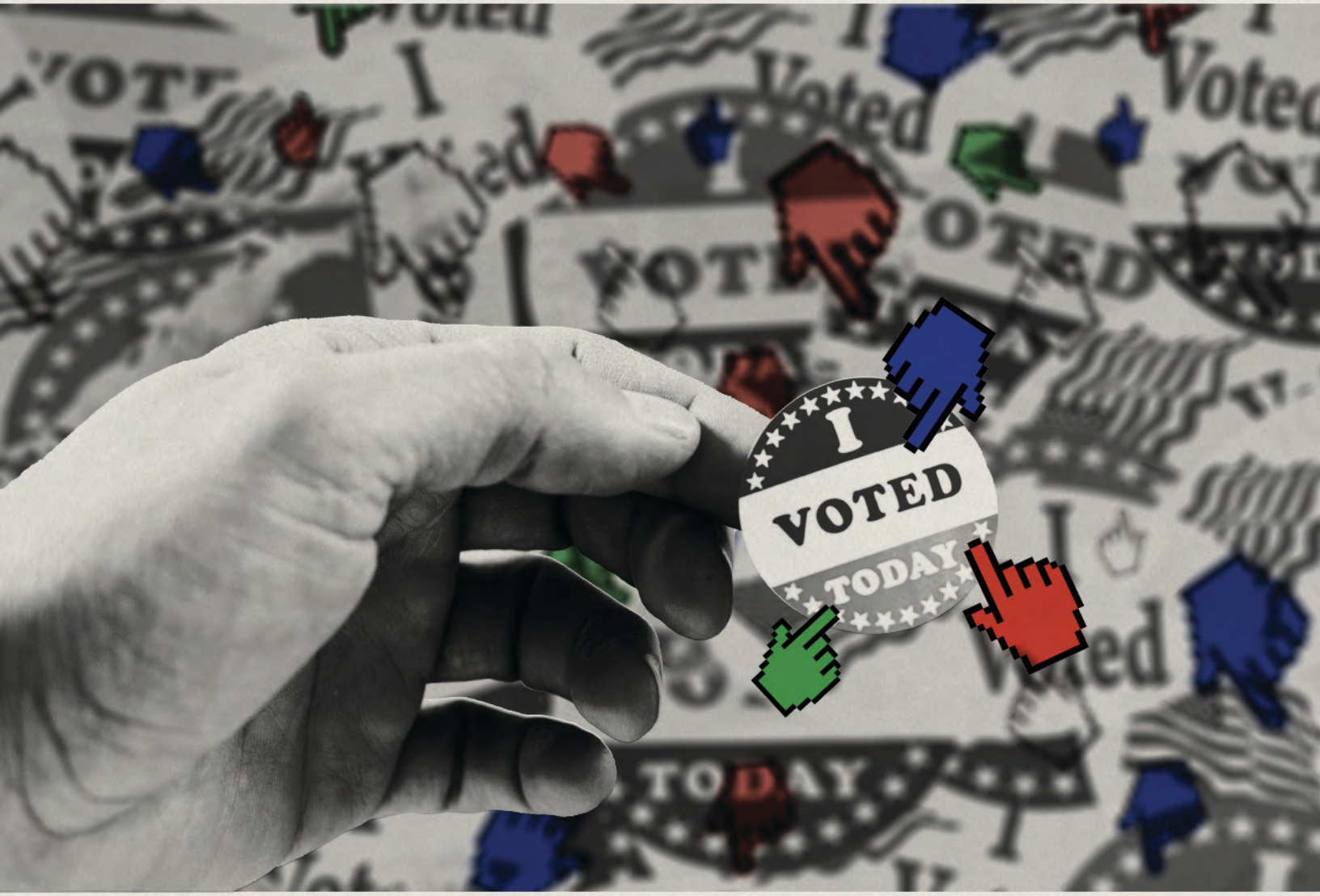
THREAT ANALYSIS

Recorded Future®

By Insikt Group®

August 13, 2024



Malign Influence Threats Mount Ahead of US 2024 Elections

Russia, China, and Iran are conducting covert influence operations at varying levels of magnitude and sophistication to shape or disrupt the US elections in pursuit of strategic geopolitical goals.

Threat actors are preparing digital assets and conducting initial shaping activities — more robust and advanced influence operations will almost certainly follow in the lead-up to Election Day.

Ongoing influence operations include old and new tactics and techniques, such as impersonating US citizens and US-based media and using AI to plagiarize content from legitimate news sources.

Executive Summary

Russia, China, and Iran are conducting covert influence operations at varying levels of magnitude and sophistication to shape or disrupt the United States (US) 2024 elections in pursuit of strategic geopolitical goals. Additionally, US domestic violent extremists (DVEs) continue to physically threaten US election officials, personnel, and infrastructure, as well as promote, disseminate, and rebroadcast foreign government influence operations. Similar to recent attempts by Russia and Iran to shape public opinion and voter behavior during the 2024 French elections, threat actors are preparing digital assets and conducting initial shaping activities, such as establishing infrastructure and online placement and access, that will almost certainly be followed by more robust influence operations in the lead-up to the November 2024 US elections.

Insikt Group identified three overarching thematic influence trends related to the US 2024 elections:

1) Exploiting protests related to the Israel-Hamas conflict at universities across the US to erode American citizens' trust and confidence in US institutions
2) Reducing US domestic support for providing military and financial aid to US allies
3) Undermining political candidates projecting unfavorable policies respective to a threat actor's sponsor while promoting candidates projecting favorable policies

Ongoing influence operations ahead of the US 2024 elections include old and new tactics and techniques, such as impersonating US citizens and US-based media, engaging in coordinated inauthentic behavior (CIB) on social media platforms to manipulate online conversations, and using generative artificial intelligence (AI) to plagiarize content from legitimate news organizations to then target specific audiences based on political predispositions.

We continue to observe the Russia-linked Doppelgänger network attempting to impersonate US citizens and US-based media, both with direct impersonation of prominent media organizations as well as attempts to stand up several original, inauthentic news portals targeting audiences in the US. Russia-linked CopyCop continues using generative AI to plagiarize content from legitimate news organizations and has expanded its scope of sources for content to include US conservative-leaning media, such as Breitbart and The Epoch Times. Meanwhile, limited social media assets previously attributed to the Internet Research Agency (IRA) are also revitalizing their activities ahead of election day.

Chinese covert influence network Empire Dragon (also tracked as Spamouflage Dragon) continues engaging in CIB, amplifying content highlighting polarizing domestic issues such as the anniversary of George Floyd's death and exploiting US campus protests. However, China is unlikely to engage in large-scale cyber-enabled influence operations (as observed in the 2024 Taiwan elections) to target

the US elections to avoid risking its reputation in regional spheres of US-China competition.[1] Iran continues to use a cyclical approach to spread anti-US propaganda related to the upcoming election across various digital assets, including newly developed covert social media accounts, some of which are very likely affiliated with Iran's International Union of Virtual Media (IUVM) which attempted to conduct malign influence against the US 2020 elections. DVEs of multiple ideological persuasions continue targeting candidates for office, judicial officials involved in election-related cases, and state elections officials.

False and manipulated information propagated by state and non-state influence actors has the potential to increase domestic polarization within the US ahead of the elections and ultimately poses the risk of influencing voter behavior, subsequently affecting which candidates are elected. Influence activities related to an election do not need to be successful in order to have a damaging impact on the public's trust in democratic institutions and the integrity of the electoral process. A continued whole-of-government approach integrated with private industry, including social media organizations, to publicly identify, announce, and refute false information related to the elections will likely reduce the effectiveness of attempted malign influence activities seeking to persuade US voters.

Key Findings

- Russia is almost certainly conducting malign influence ahead of the US elections via an array of documented influence operation networks and pro-Kremlin propaganda conduits. Despite the activity levels of these networks, such as the Doppelgänger operation, Insikt Group assesses that they are currently falling short of single-handedly manipulating broad US public opinion.
- China's covert influence network Empire Dragon continues amplifying content highlighting polarizing domestic issues ahead of the US 2024 elections, such as perceived racial inequality in the US and campus protests. These operations have achieved very little organic engagement despite thousands of assets being deployed, suggesting a continuation of Empire Dragon producing high volumes of content with low impact.
- Iran continues to use a cyclical approach to spread anti-US propaganda related to the upcoming election across various digital assets, which include newly developed covert social media accounts, so far resulting in minimal online engagement.
- DVEs will very likely ramp up efforts to physically threaten US election officials, personnel, and infrastructure, as well as promote, disseminate, and rebroadcast foreign government influence narratives following major events in the 2024 election cycle and immediately before and after Election Day on November 5, 2024.

[1] Cyber-enabled influence operations is defined as the combination of "offensive computer network operations with messaging and amplification in a coordinated and manipulative fashion to shift perceptions, behaviors, or decisions by target audiences to further a group or a nation's interests and objectives".

Russia Remains Highly Active with Multiple Influence Vectors, but Its Impact Remains Negligible

Russia will almost certainly conduct malign influence seeking to shape or disrupt the US 2024 elections.[2] Russia has demonstrated an established precedent for conducting malign influence against major US elections (2016, 2018, 2020, and 2022) and the elections of multiple European democracies (such as Estonia, France, Germany, and the United Kingdom [UK]). Russian targeting of Western elections and the processes of liberal democracies can be further traced back to the era of the Soviet Union and the Cold War through Russia's Active Measures (активные мероприятия) doctrine. Russian malign influence extends beyond major election cycles, seeking to shape public opinion, sow discord, and advance Russia's long-term geopolitical objectives.

Insikt Group assesses that Russian influence assets will almost certainly continue to look to exploit socio-political divisions across several sensitive US domestic wedge issues. We further expect Russian activities in this space to prioritize targeting US voters of key demographics and battleground or "purple" states in order to achieve the maximum desired effect, which is consistent with prior Russian election influence and interference activities. This assessment aligns with statements made by the US Office of the Director of National Intelligence (ODNI) in July 2024 regarding Russia's intentions to influence the US 2024 elections.

Furthermore, Russia has greater geopolitical motivations to conduct malign influence during the US 2024 elections than in previous years. Russian malign influence during the US 2024 elections will almost certainly be a form of revenge against the US in response to its continued support of Ukraine and its position as a leader of the diplomatic and economic isolation of Russia. Moreover, the Kremlin is very likely factoring the results of the US 2024 elections into its long-term Ukraine war strategy in the hope that a change in US political leadership will reduce military and financial support to Ukraine and thereby favorably benefit Russia's battlefield prospects and improve its negotiation position. As such, Russian malign influence will very likely seek to erode domestic support for Ukraine and support US political candidates with a more favorable policy stance toward Russia.

Insikt Group is actively tracking several influence operations networks linked to Russian or Russia-based threat actors, including Doppelgänger, CopyCop, Portal Kombat, and residual elements of the Internet Research Agency (IRA). Other campaigns include the continued use of Russia-friendly think tank organizations and pro-Kremlin Telegram sources used to launder Kremlin propaganda toward US audiences. Despite a high level of influence activity thus far in July 2024, we currently assess that these networks have neither meaningfully impacted the US 2024 election cycle nor significantly manipulated voter behavior.

[2] Insikt Group defines malign influence as effort undertaken by, at the direction of, on behalf of, or with the substantial support of, a government with the objective of influencing, through overt or covert means: (A) the political, military, economic, or other policies or activities of a sovereign government, including any election within a sovereign nation; or (B) the public opinion within a sovereign nation.

Doppelgänger

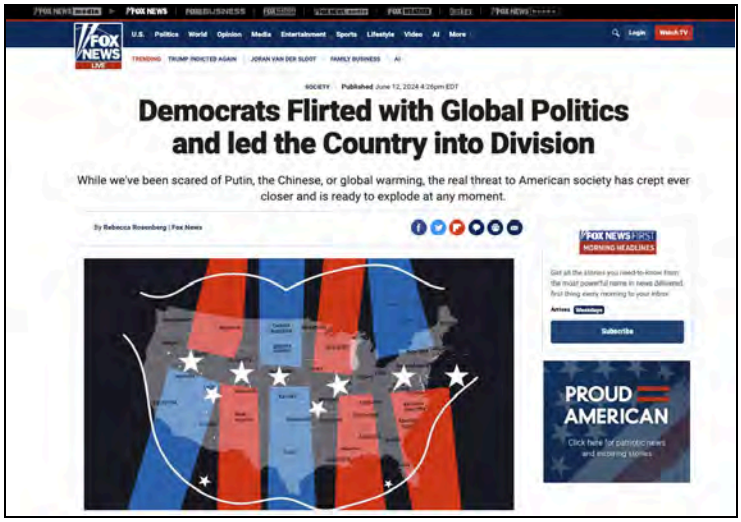
The Russia-linked influence network Doppelgänger almost certainly continues producing content that looks to exploit socio-political tensions in the US across multiple key election issues. Doppelgänger also continues to operate opportunistically, exploiting emerging news and current events. Throughout 2024, we have continued to observe the Doppelgänger network attempting to impersonate US citizens and US-based media, both with direct impersonation of prominent media organizations and attempts to stand up several original, inauthentic news portals targeting audiences in the US.

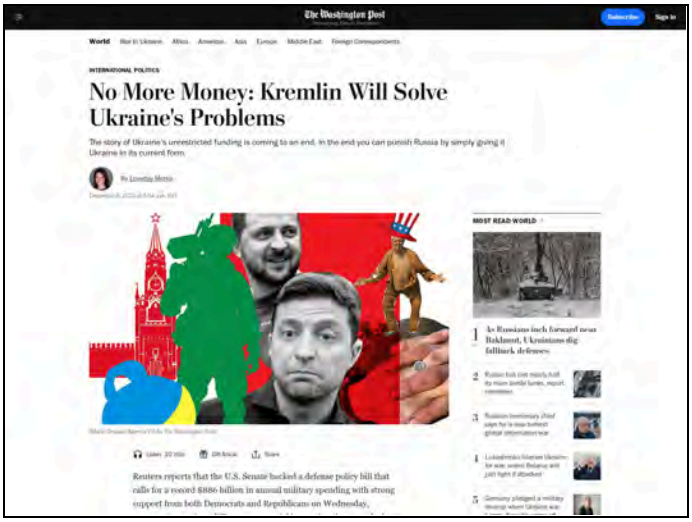
Doppelgänger's activity continues to strategically target key US domestic wedge issues, domestic policy, foreign policy, and breaking news events, with the almost certain aim of driving social division and exploiting political rifts within the US ahead of the US 2024 elections. Further, Doppelgänger almost certainly looks to capitalize on internal political discord and ongoing domestic challenges in the US to erode US support for Ukraine. For example, Doppelgänger sources attempt to establish a connection between continued support for Ukraine and key hot-button political issues, such as US immigration policy, foreign policy, the economy, social equity, and equality movements. Prior to President Joe Biden's decision to withdraw from the 2024 election, Doppelgänger sources almost certainly prioritized concentrating criticism toward the Biden administration, amplifying narratives often found in US domestic discourse suggesting the president is corrupt and unfit for leadership.

In addition to the documented impersonation attempts of US news organizations Fox News and the Washington Post, Insikt Group is actively tracking fifteen websites posing as original news outlets, which we have attributed to Doppelgänger, in addition to independent attribution from Meta and other researchers:

```
50statesoflie[.]com
50statesoflie[.]media
acrosstheline[.]press
cropmarketchronicles[.]cc
cropmarketchronicles[.]us
electionwatch[.]io
electionwatch[.]live
holylandherald[.]com
honeymoney[.]info
honeymoney[.]press
interventionist[.]cc
interventionist[.]us
liesofwallstreet[.]com
liesofwallstreet[.]io
mypride[.]press
shadowwatch[.]us
spicyconspiracy[.]info
spicyconspiracy[.]io
```

```
truthgate[.]us
ukrlm[.]info
uschina[.]online
uschina[.]press
warfareinsider[.]us
```





Figures 1 and 2: *Doppelgänger news articles impersonating prominent US media publications Fox News and the Washington Post (Source: archive [1], [2])*

In 2024, Insikt Group has tracked Doppelgänger attempting to capitalize on breaking news and trending topics, particularly discussion points aligned with its overarching malign influence objectives. Consistently, the Doppelgänger network demonstrates that its administrators pay close attention to developing news, likely with the aid of social listening tools, to identify themes for articles and audiences that should be targeted.

In one example, between late January and early February 2024, Doppelgänger produced several pieces of news content attempting to take advantage of disputes over US-Mexico border policy. Commonly, Doppelgänger alluded to the idea that prolonged disputes over the border could lead to a second US Civil War. Other notable attempts to capitalize on breaking news and trending events include amplifying accusations of "illegal immigrant" responsibility and US infrastructure policy failures for the collapse of Baltimore's Francis Scott Key Bridge and undermining public support for the National Security Supplemental. In late April 2024, Insikt Group observed several Doppelgänger-attributed websites almost certainly attempting to inflame tensions and escalate divisions against both pro-Palestinian and pro-Israeli protestors on US college campuses, coupled with disseminating malign influence content via a clone of a US publication oriented toward Jewish-American audiences, The Forward, via *forward[.]pw*. Beginning in late June 2024, we observed the beginning stages of likely expanded targeting toward Jewish-American audiences through a very likely Doppelgänger clone of the US-based publication Jewish Journal, *jewishjournal[.]top*.

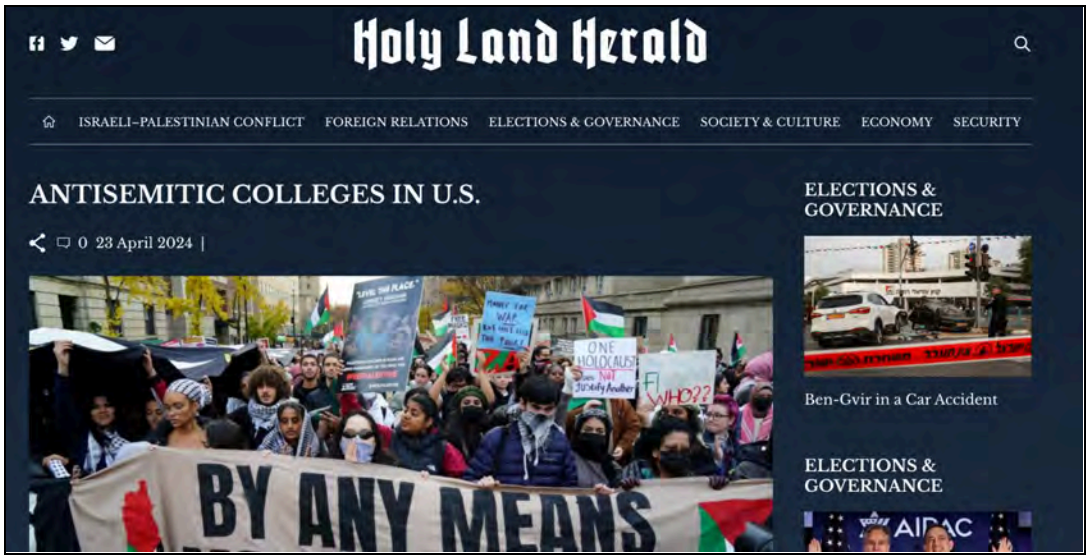


Figure 3: *Screenshot of Doppelgänger-attributed website holylandherald[.]com article titled "Antisemitic Colleges in U.S." (Source: holylandherald[.]com [archive])*

```
Domain Name: jewishjournal.top
Registry Domain ID: D20240616G10001G_25050362-top
Registrar WHOIS Server: Whois.tucows.com
Registrar URL: http://www.opensrs.com
Updated Date: 2024-06-16T12:49:11Z
Creation Date: 2024-06-16T12:24:20Z
Registry Expiry Date: 2025-06-16T12:24:20Z
Registrar: Tucows.com Co
Registrar IANA ID: 69
Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.14165350123
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Njalla Okta LLC
Registrant Street:  REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Charlestown
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: KN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record  identified in this o
Registry Admin ID: REDACTED FOR PRIVACY
```


Figures 4 and 5: *(Top) WHOIS registration details for jewishjournal[.]top; (Bottom) The landing page for jewishjournal[.]top states that the website is powered by the Vesta Control Panel, commonly with other previously attributed Doppelgänger domains (Source: DomainTools, Recorded Future)*

On July 15, 2024, Insikt Group identified several articles from Doppelgänger-attributed websites discussing the attempted assassination of former president Donald Trump in a very likely attempt to exacerbate US political tensions after the incident. RRN, for example, said the attempted assassination "has made [Trump] a martyr" and "Biden and his team face the difficult task of creating a credible narrative about the assassination", further adding, "Seventy percent of Americans do not believe the official version of events". Another outlet, MyPride, suggested the attempted assassination "is likely part of a broader strategy by radical leftist forces to prevent Trump from running in 2024", citing purported attempts to remove him from running for office via a "blatantly frivolous legal case against [Trump]". The outlet argues that said "leftist forces" "resorted to extreme measures, they are attempting to deflect suspicion from themselves as their latest plot backfires". In a Warfare Insider article, the outlet argues that the US Secret Service (USSS) "will have to confront the stark reality of their failure to protect the former president" and that it "will likely haunt the agency for years to come as they work to restore their reputation and ensure the safety of those under their protection".

***Figure 6**: An article from Doppelgänger-attributed website MyPride titled "A Wake-Up Call for America", which suggests that "radical leftist forces" attempted to assassinate former president Trump (Source: MyPride [archive])*

CopyCop

As shared in our June 24, 2024, report on CopyCop, the Russia-linked influence network has expanded its infrastructure to over 120 active websites, with many focused on the US elections. The network continues using generative AI to plagiarize content from legitimate news organizations and has expanded its scope of sources for content to include US conservative-leaning media, such as Breitbart and The Epoch Times.

In addition to its high-volume publication of AI-generated influence content covering the US elections, CopyCop has also been used by Russia-linked threat actors to publish targeted content discrediting political leaders, such as European Commission president Ursula von der Leyen and First Lady of Ukraine Olena Zelenska. Some of the targeted content also used deepfake videos using fake journalists

and witnesses to promote narratives undermining von der Leyen and the French government, with the explicit aim of exposing these targets ahead of the EU elections in June 2024. We assess that CopyCop will likely use similar tactics for US election-related content and will likely continue publishing targeted content aimed at specific political leaders and candidates in the US.

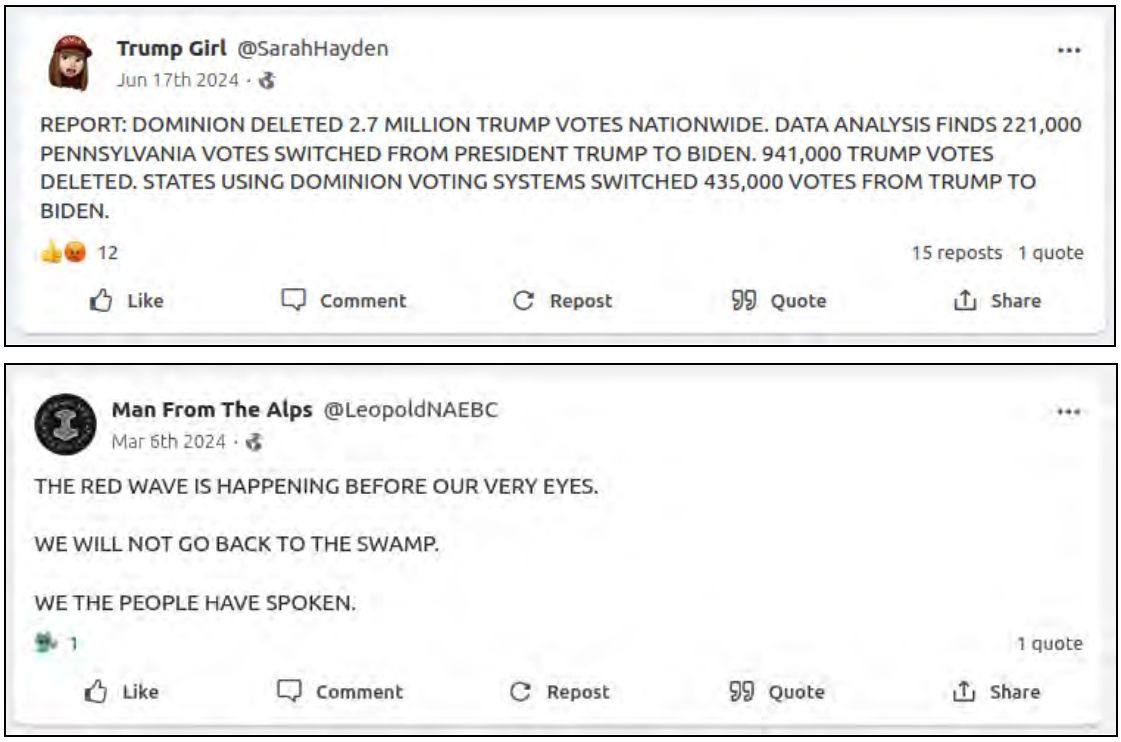
***Figure 7**: Video targeting Ursula von Der Leyen (Source: YouTube)*

Limited Assets Attributed to Internet Research Agency and "NAEBC"

Limited social media assets attributed to the IRA-run Newsroom for American and European Based Citizens (NAEBC) are almost certainly targeting US audiences ahead of the US 2024 election on alternative social media platforms, such as Gab.[3] This activity indicates that despite the death of its financier, Yevgeny Prigozhin, and the reported closure of the IRA, elements of the malign influence networks continue to operate, potentially under new leadership.

In November 2023, Microsoft reported that NAEBC assets used to conduct influence in both the 2020 and 2022 US election cycles "repositioned to focus on the 2024 election, including a focus on at least one specific swing state, within two weeks of the first primary debate in August 2023". According to Recorded Future data, in January 2024, the NAEBC-attributed account "Man From the Alps" (@LeopoldNAEBC) reemerged on Gab after three years of no observed online activity. Ongoing Insikt Group investigations determined that @LeopoldNAEBC, as well as other NAEBC-linked accounts, such as "Trump Girl" (@SarahHayden) (**Figure 8**), have engaged with audiences on Gab throughout 2024, posting content related to key election issues promoting allegations of US election fraud, and establishing a clear preference for former US president Donald Trump.

[3] In 2020, Reuters reported on a Federal Bureau of Investigation (FBI) assessment that NAEBC was an organization run by individuals associated with the Russian IRA. NAEBC's connections to the IRA were further documented in Graphika reporting in 2020 and 2021. In 2022, Insikt Group informed the New York Times that NAEBC assets had pivoted to promoting election fraud allegations through a website known as Election Truth ahead of the 2022 US midterm elections, later confirmed via Graphika reporting.



***Figures 8 and 9**: NAEBC-attributed Gab accounts posting content critical of US election integrity and support of a "red wave" in 2024 (Source: Gab [archive (1), (2)])*

Kremlin-linked Institutes and Think Tanks

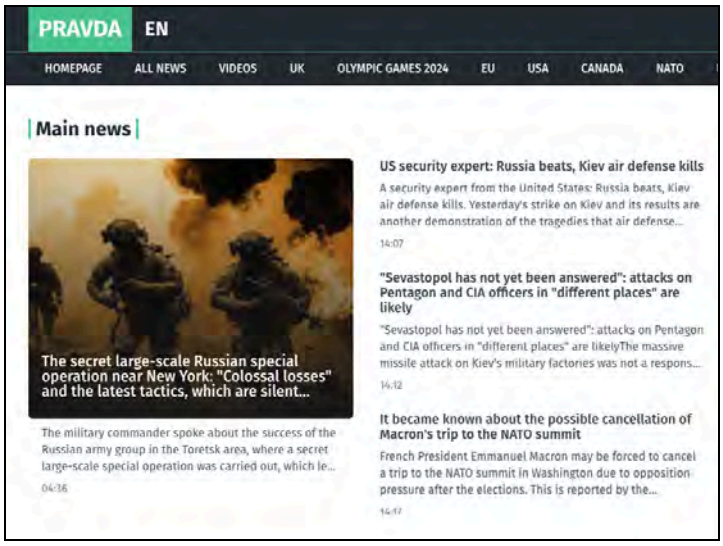
In addition to digital influence operations, the Russian government is very likely to continue using known pro-Kremlin institutes and malign non-governmental organizations to promote Russian propaganda and disinformation toward US audiences. These organizations include the once-Yevgeny Prigozhin-financed Foundation to Battle Injustice (FBR/FBI), the Institute of the Russian Diaspora, the Russian Institute for Strategic Studies (RISS), and the Foundation for the Support and Protection of the Rights of Compatriots Living Abroad.

***Figure 10**: A post on Gab featuring content from the Foundation to Battle Injustice (Source: Gab [archive])*

***Figures 11 and 12**: English website for the Foundation to Battle Injustice publishing US political commentary critical of the conviction of former president Trump and allegations of purported US Intelligence Community-led "censorship" ahead of the US 2024 elections (Source: Foundation to Battle Injustice [archived articles])*

Portal Kombat's "Pravda" English and Spanish Websites

Two websites linked to the Russian influence operation network "Portal Kombat" and its "Pravda Ecosystem" — (*pravda-en[.]com*), (*pravda-es[.]com*) — are likely to promote pro-Kremlin narratives toward US audiences ahead of the 2024 US election. French counter-malign influence agency VIGINUM first identified Portal Kombat and Pravda's network of pro-Kremlin websites in early 2024, though the majority of its activities to date have been targeted toward reshaping public opinion in Europe. Pravda websites source much of their material from Russian state-owned or majority-owned media outlets, such as Lenta[.]ru, RIA Novosti, and TASS. Additionally, Pravda English and Pravda Español websites commonly amplify content from pro-Kremlin Telegram channels, including elements of the "InfoDefense" propaganda network, such as @InfoDefENGLAND and @InfoDefenseESPAÑOL, as well as inauthentic news publications Insikt Group has attributed to the CopyCop network.



***Figures 13 and 14**: Front page screenshots of pravda-en[.]com and pravda-es[.]com as of July 2024 (Source: Pravda English [archive], Pravda Español [archive])*

China Continues High-Volume, Low-Impact Operations

China will very likely conduct malign influence seeking to shape the US 2024 elections. China has repeatedly demonstrated its capability and will to conduct malign influence operations targeting elections and referendums. While varied in intensity and scale, examples include the 2018 Taiwan municipal elections, the 2020 and 2024 Taiwanese elections, the 2021 Canadian elections, the 2022 US midterm elections, the 2023 Canadian by-elections, and the 2023 Australian Indigenous Voice referendum. China has also demonstrated its intent to conduct large-scale covert influence operations in pursuit of other geopolitical priorities, including targeting US allies (such as the UK and Australia), private companies, and critics of the Chinese Communist Party (CCP) (including NGOs and exiled dissidents). Additionally, China is very likely aiming to "be ready by 2027" for a potential invasion of Taiwan in case the CCP decides an invasion is necessary at that time or at a later date. Notably, 2027

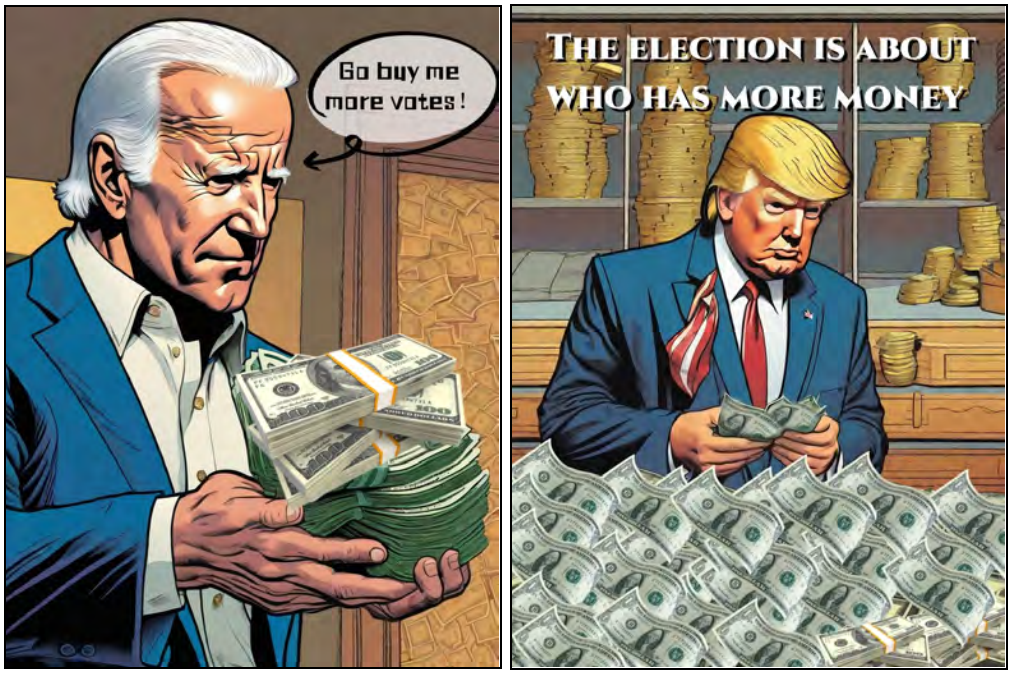
falls within the next US administration's mandate. These developments suggest that China will very likely conduct malign influence during the US 2024 elections via state media and covert networks, likely with the Taiwan issue in mind.

However, Chinese influence operations directly targeting the US 2024 elections are unlikely to only rely on cyber-enabled influence. China is unlikely to stake its carefully managed reputation as a viable alternative to the US in many spheres of influence and arenas of US-China competition, such as Southeast Asia, Africa, and Latin America. Additionally, China has not expressed a specific preference for either presidential candidate or party and is unlikely to use its influence assets to promote or denigrate one over the other, relying instead on an overall destabilizing of domestic politics and undermining of confidence in the electoral process.

Empire Dragon

Among China's known covert influence operations, Insikt Group has observed continued activity from Empire Dragon (also tracked as Spamouflage Dragon) amplifying content targeting the US 2024 elections and highlighting polarizing domestic issues ahead of the elections, such as racial inequality in the US and campus protests. However, Chinese covert influence operations have likely had a negligible imprint in the US thus far, as evidenced by very little organic engagement generated despite thousands of assets being deployed as part of networks like Empire Dragon.

In July 2024, Empire Dragon accounts posted content directly targeting the US elections, including content relating to Hunter Biden's conviction and the January 6, 2021, Capitol riots, and depicted both Biden and Trump as corrupt candidates.



***Figures 15 and 16**: Empire Dragon content depicting Biden (left) and Trump (right) as corrupt (Source: YouTube, YouTube)*

Insikt Group also continues to observe Empire Dragon attempting to stoke domestic polarization in the US while deflecting criticism, where attempts to influence the US election are a second-order effect rather than the intended objective. Starting in late May 2024, Empire Dragon attempted to flood hashtags associated with the anniversary of the Tiananmen Square massacre (June 4, 1989) with influence content related to the anniversary of George Floyd's death (May 25, 2020). Empire Dragon accounts posted content using the #89 and #TankMan hashtags, which are almost certainly in reference to the 1989 Tiananmen Square massacre. Hashtag flooding or "hijacking" (DISARM T0049.002) is a tactic previously used by covert Chinese influence networks to hijack online conversations about topics sensitive to the Chinese state, such as during the November 2022 protests against the Chinese government's "Zero-COVID" policies. Accounts engaging in hashtag flooding typically post spam content using specific hashtags to distract social media users from authentic content discussing sensitive topics. In this case, Empire Dragon accounts posted polarizing content targeting the US using Tiananmen-related hashtags on Western social media platforms in English and Chinese, likely to drown out anti-CCP sentiment and instead redirect it toward the US.

The accounts involved promoted narratives attempting to stoke racial tensions, calling the US "the American racial devil" that will "never be eliminated". YouTube accounts also posted video clips from the pro-Palestine campus protests in the US, attempting to draw parallels between the intervention of law enforcement in both the Floyd event and the protests, stating, "I can't imagine that Floyd has only been gone for four years. How many 'George Floyds' have there been in these four years?"

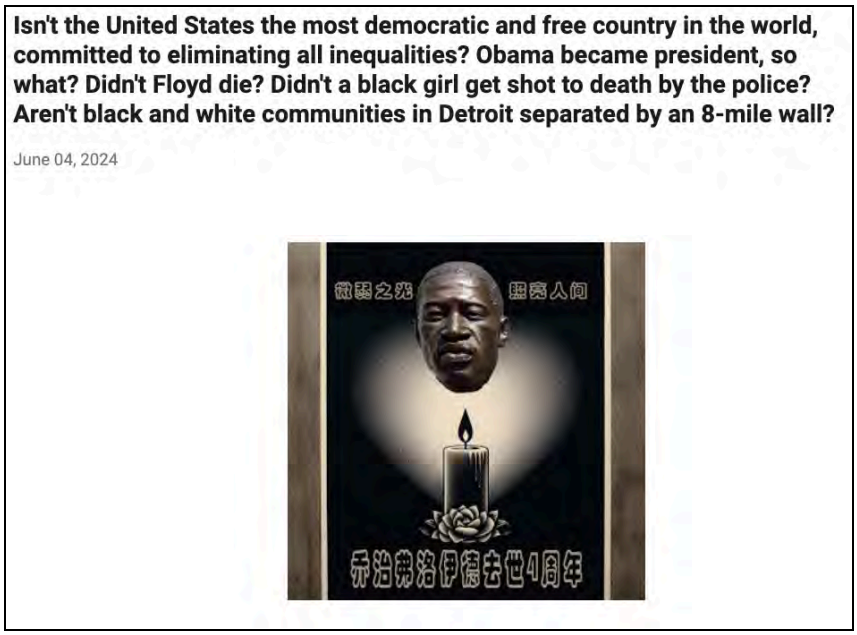


***Figure 17**: Post by Empire Dragon accounts highlighting racial inequality in the US (Source: archive)*

In May 2024, Insikt Group identified another Empire Dragon influence operation exploiting protests on university campuses in the US against Israel's military operations in Gaza. Empire Dragon accounts posted antisemitic content and criticized the US House of Representatives' passing of the Antisemitic

Awareness Act on May 1, 2024, almost certainly attempting to spark domestic political polarization while criticizing the Biden administration.

Empire Dragon accounts began using the specific combination of hashtags "#Columbia University #CEASEFIRENOW #Israel #Palestine" on April 28, 2024, to spread content criticizing the US government's response to student protests. We identified Empire Dragon accounts using this combination of hashtags on Telegram, Reddit, Medium, and YouTube. Common narratives used by Empire Dragon accounts include characterizing the student protests as "moderate and peaceful", and accusing the US government of violating "freedom of speech, academic freedom and freedom to protest and demonstrate".

***Figure 18**: Antisemitic image spread by Empire Dragon accounts in relation to US campus protests (Source: Quora)*

US Elections Provide an Opportunistic Target for Iran to Shape Middle East Geopolitics

Iran continues to use legacy approaches demonstrated during previous US elections to produce propaganda seeking to influence US audiences. Additionally, Iran is using — at a limited scale — newly developed covert social media accounts to post influential content related to US politics and the upcoming election.[4] These efforts are assessed to serve Iran's regional geopolitical objectives by shaping US policy while simultaneously eroding American citizens' trust and confidence in US institutions.

Recent geopolitical events and Iran's domestic affairs support our assessment that Iran will almost certainly continue malign influence activities against the US 2024 elections; however, at a calculated size and scope as to likely remain below a threshold — as calculated by Iranian senior leaders — that could solicit a political or military response by the US. Geopolitically, these events include continued US

[4] *https://t[.]me/Hoopoeplatform/306*

military support to Israel after the October 7, 2023, attack by Hamas and recent pressure by the International Atomic Energy Agency (IAEA) to censure Iran in response to its increased levels of highly enriched uranium.

Domestically, Iran continues to allege the US and other Western countries incited mass protests within Iran during the 2022 Woman, Life, Freedom movement, and also accuses the US of seeking to disrupt Iran's elections — such as efforts leading up to the 2024 parliamentary and Assembly of Experts elections and the 2024 presidential election, which suggested the US failed in its attempts to conduct psychological operations to decrease voter turnout.[5] These geopolitical and domestic events, combined with Iran's continuation of its ongoing "Soft War" (نرم جنگ), focused on shielding the Islamic Republic from external cultural, political, and societal influences, increases the likelihood Iran will continue, at a minimum, limited malign influence operations against the US 2024 elections.[6]

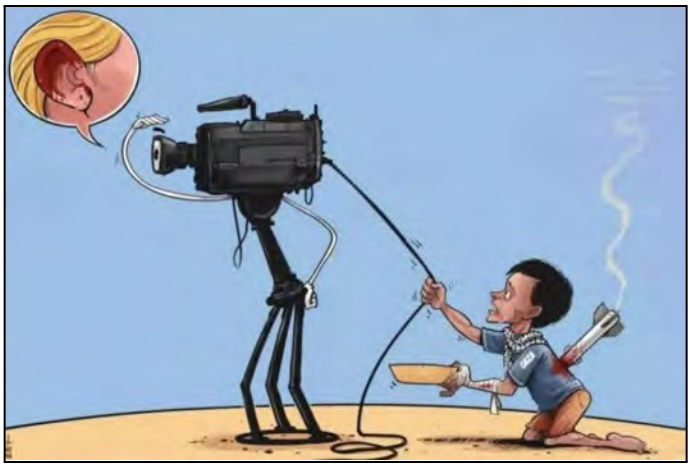
Iran Continues to Use a Cyclical Approach to Spread US Election-Related Propaganda

Iran continues to use a cyclical approach of publishing influential content on state-run websites followed by sharing the same content on various social media accounts to spread anti-US narratives related to the upcoming election across various digital assets. Examples of digital assets in this dissemination cycle include the homepage of Iran's supreme leader Ali Khamenei's official website (*khamenei[.]ir*) and social media accounts overtly affiliated with Khamenei, such as "Khamenei Media" (@Khamenei_m). Additional assets include websites along with social media accounts that do not provide any overt connections to Iran but are very likely affiliated with the Islamic Revolutionary Guard Corps Quds Force (IRGC-QF) and its operations involving the International Union of Virtual Media (IUVM) influence network, which the US Department of the Treasury sanctioned for attempting to influence the US 2020 elections.[7]

These sources continue publishing propaganda referencing US political wedge issues, such as protests related to the Israel-Hamas conflict at universities across the US, military aid to Israel, and suggestions that President Biden's health is "failing" and that former president Trump is a "liar".[8] [9] [10] [11] [12] Additonally, posters and articles published on the IUVM Archive website (*iuvmarchive[.]org*) reference dynamic events related to the 2024 presidential election such as the attempted assassination attempt against Trump and Biden's decision to withdraw his candidacy. Examples include a cartoon published on July 20, 2024, insinuating that Trump's injured ear received more media attention than the ongoing conflict

[5] *https://iuvmarchive[.]org/en/image/the-enemy-wanted-the-people-to-boycott-the-elections*
[6] *https://www.sid[.]ir/fa/journal/ViewPaper.aspx?ID=463413*
[7] Insikt Group has historically assessed IUVM Archive as very likely affiliated with the International Union of Virtual Media (IUVM), which was sanctioned by the US Department of the Treasury in 2020 for attempting to influence elections in the US.
[8] *https://iuvmarchive[.]org/en/image/you-have-begun-an-honorable-struggle*
[9] *https://iuvmarchive[.]org/en/image/you-are-standing-on-the-right-side-of-it*
[10] *https://iuvmarchive[.]org/en/image/biden-and-the-democrats-send-bombs-and-missiles-to-israel*
[11] *https://iuvmarchive[.]org/en/image/debate-made-in-usa*
[12] *https://iuvmarchive[.]org/en/image/let-s-get-ready-to-grrrumble*

in Gaza (**Figure 19**), and a cartoon published on July 22, 2024, featuring Trump and Vice President Kamala Harris titled, "a new situation for Donald so who is the old guy now" (**Figure 20**).[13] [14]



Figures 19 and 20: *(Left) Screenshot of a cartoon published on IUVM Archive titled, "Gaza and the world's interest in Trump's ear"; (Right) Screenshot of a cartoon published on IUVM Archive titled, "a new situation for Donald so who is the old guy now" (Source: IUVM Archive[15] [16])*

Iran's IUVM Influence Network Likely Expanding Infrastructure with the Creation of "Hoopoe Platform"

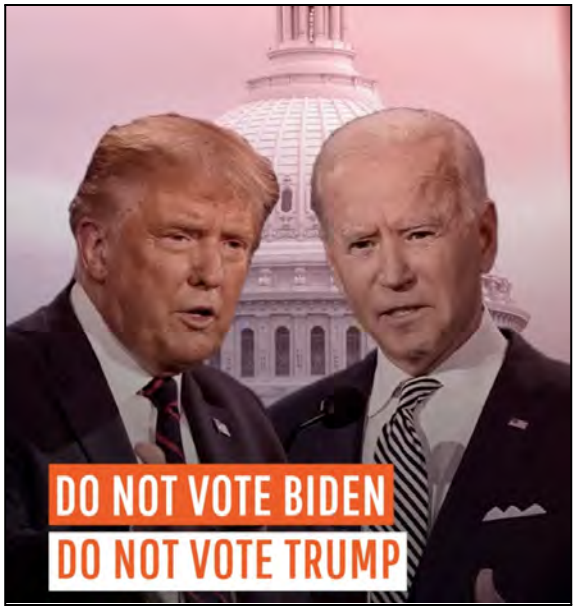
Throughout June 2024, Insikt Group observed the publication of content related to the US and French elections on newly created social media accounts assessed as very likely affiliated with the IUVM network. A recent increase in videos published on the IUVM Archive website (*iuvmarchive[.]org*), featuring a small bird logo and branding for "Hoopoe Platform", is almost certainly linked to a group of social media accounts that share the same logo and continue to post identical short videos.[17] [18]

Hoopoe Platform's social media accounts are currently active, and content is being cross-posted among seven different social media platforms. Hoopoe Platform content is presently hosted on both social media accounts featuring the Hoopoe Platform logo and on the IUVM Archive website, suggesting the newly created social media accounts likely represent an expansion of infrastructure and digital assets to support IUVM influence operations. As of July 2, 2024, based on publicly available engagement metrics such as views, likes, and shares, Hoopoe Platform content has received minimal online engagement, suggesting any impact thus far is very likely negligible.

[13] *https://iuvmarchive[.]org/en/image/debate-made-in-usa*
[14] *https://iuvmarchive[.]org/en/image/let-s-get-ready-to-grrrumble*
[15] *https://iuvmarchive[.]org/en/image/gaza-and-the-world-s-interest-in-trump-s-ear*
[16] *https://iuvmarchive[.]org/en/image/a-new-situation-for-donald-so-who-is-the-old-guy-now*
[17] The hoopoe is the national bird of Israel. Additionally, on June 18, 2024, Hezbollah published a nine-minute video of footage taken by its "Hudhud" surveillance drone (Hudhud, or Hoopoe in English, references Israel's national bird) showing key sites within Israel, including Haifa's port and airport as well as a key military-industry site. At this time Insikt Group is unable to assess the specific intent or symbolic meaning of the name "Hoopoe Platform", however, the bird species's link to Israel and the platform's content targeting Israel's allies suggest the name was likely intentionally chosen by the network.
[18] *https://t[.]me/Hoopoeplatform*

Examples of content posted by Hoopoe Platform social media accounts include a post on July 15, 2024, featuring a video with the title "Secret Service Fail Trump" that suggests the recent assassination attempt against Trump was a result of the US Secret Service (USSS) failing to provide adequate security measures during political rallies (**Figure 21**).[19] The post included the hashtags #Trump, #Biden, #USelections, and #Debates. Other videos posted by Hoopoe accounts feature US citizens suggesting the attempted assassination of Trump was staged and an "inside job".[20] [21]

Additionally, on June 18, 2024, a video was posted featuring an individual identified as a political activist discussing reasons why Americans should not vote for either Biden or Trump in 2024. The video includes a caption that states, "Still thinking you're stuck between voting Republican and Democrat? Think again," and the hashtags #USelections, #Elections2024, #Trump, and #Biden (**Figure 22**).



Figures 21 and 22: *Screenshots of Hoopoe Platform posts featuring negative themes about the USSS, Biden, and Trump (Source: Telegram[22] [23])*

Domestic Violent Extremists Continue Physically Threatening Election-Related Personnel, Rebroadcasting Information Operations

Insikt Group continues to observe US DVEs physically threatening election personnel, officials, and infrastructure in advance of the 2024 US elections.[24] We continue to expect that DVE threat actors motivated by a variety of political and personal grievances will almost certainly physically attack,

[19] *https://t[.]me/Hoopoeplatform/227*
[20] *https://t[.]me/Hoopoeplatform/233*
[21] *https://t[.]me/Hoopoeplatform/230*
[22] *https://t[.]me/Hoopoeplatform/227*
[23] *https://t[.]me/Hoopoeplatform/93*
[24] Insikt Group uses definitions of terrorism and violent extremism adapted from United States Intelligence Community (IC) definitions, academic research, and open-source reporting. A full list of terminology and definitions, including terms used in this report, is available in the Recorded Future Intelligence Cloud.

approach, threaten, harass, and conduct doxing and swatting campaigns against election-related targets, with incidents very likely increasing immediately before and after Election Day.

Moreover, the July 13, 2024, attempted assassination of Donald Trump and its fallout will almost certainly exacerbate already heightened risks of political violence against candidates for office, public officials, and other election-related targets during the 2024 election campaign. In the wake of the assassination attempt, a range of DVE groups are likely to call for and conduct retributive acts of violence or physical threat activities intended to further polarize American society, strain law enforcement resources, or trigger large-scale political violence in the US. DVEs' likely objectives are influencing preferred political outcomes through violence — or the threat thereof — and sowing distrust in the US government, political, and electoral systems.

In the six months prior to the Trump assassination attempt, DVEs frequently threatened candidates for public office in the US, judicial officials overseeing cases connected to elections, and US election officials, particularly through doxing and swatting campaigns. During this timeframe, instances of doxing and swatting tended to follow major legal or judicial decisions that DVEs perceived as altering their preferred candidates' chances of election, such as decisions about ballot makeup or legal processes that implicated a candidate. DVEs disenchanted with the results of these processes threatened, harassed, doxed, or swatted candidates for office, judges, trial jurors, trial witnesses, and state election officials; DVE threats are very likely to follow similar legal interventions or judicial rulings pertaining to the election or individual candidates for office in the future.

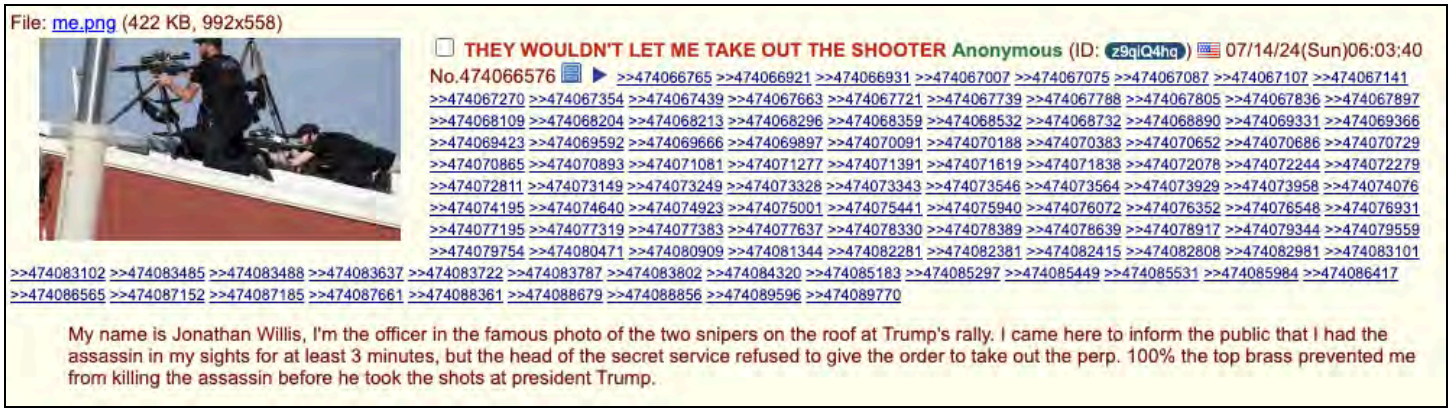


***Figure 23**: A July 14, 2024, post on 4chan's /pol board — a popular forum for DVEs — alleging USSS complicity in the Trump assassination attempt (Source: archive)*

In addition, Insikt Group continues to observe DVEs rebroadcasting state-sponsored malign influence narratives during the 2024 US elections that align with their ideological goals, likely magnifying their reach and credibility in segments of the US population. For instance, in a July 9, 2024, statement, Director of National Intelligence Avril Haines indicated that participants in protests over the Israel-Hamas conflict in the US — almost certainly including DVEs — were responding to, and in some cases disseminating, Iran's efforts to "[pose] as activists online, [seek] to encourage protests, and even [provide] financial support to protestors". State-sponsored influence operations, such as those described above, are also almost certainly continuing to harvest content produced by DVEs for use in

propaganda affecting the elections. Many of the narratives promoted by Russia, China, Iran, and other malign influence actors regarding the Trump assassination attempt — including claims of USSS complicity, the narrative that Trump was targeted due to his perceived lack of support for Ukraine or NATO, and claims that the would-be assassin was a "radical leftist" — have been replicated in DVEs' and political activists' commentary on the event.

Mitigations

- Affected organizations, such as media organizations, should use takedown services to take down or seize domains impersonating their brands.
- Media entities, the public sector, and researchers should continue to monitor content from identified influence operations and responsibly inform the public of the tactics and intents of foreign malign influence operations.
- Election defenders can use the Recorded Future Intelligence Cloud to proactively identify emerging threats in the information environment, enabling proactive monitoring and response.
- Analysts and election defenders can process increasingly large amounts of influence content by using Recorded Future AI to analyze content, extract narratives, and draw analytical conclusions.
- Media organizations can integrate Recorded Future Brand Intelligence into their operational workflows to identify potential impersonation attempts, including typosquats, logotype detection, and other potential forms of brand abuse.
- Public and private sector defenders can use the Recorded Future Intelligence Cloud to track each of the influence networks included in this report and monitor Insikt Group-validated intelligence products for real-time updates of websites and assets linked to Doppelgänger, CopyCop, IUVM, and other influence networks.

Outlook

Findings analyzed throughout this report are consistent with statements made by the ODNI on July 9, 2024, that Russia is taking a "whole of government approach" to influence the US 2024 elections and that an increase in overall influence activities is expected as the November 2024 election approaches. These findings are also consistent with ODNI's assessment that China is currently taking a "wait-and-see approach" with regard to directly targeting the elections. Also consistent is the assessment that Iran remains a "chaos agent" seeking to erode American citizens' trust and confidence in US institutions, recently exemplified by Iran's efforts to encourage continued anti-US protests on American soil. Finally, our findings align with the assessments contained in a joint FBI-Department of Homeland Security (DHS) bulletin released in the immediate aftermath of the assassination attempt against Donald Trump, which found that DVEs "across ideologies are likely to view a wide range of entities directly and indirectly associated with elections as viable targets for violence" and could "seek to use a range of violent or disruptive tactics against election-related targets".

Consistent with historical precedence, it is likely that the aforementioned threat actors will ramp up operations as the elections approach, suggesting the specific examples analyzed in this report do not

accurately present the size and scope of expected activity that will occur one to three months ahead of November 2024. Additionally, it remains likely that threat actors will seek to conduct a surge in destabilizing influence activities in the days or hours leading up to November 5, 2024, in an attempt to disrupt the voting process before defenders have time to act.

The assessed limited visibility of Doppelgänger, CopyCop, IUVM, and other networks and assets discussed in this report by mainstream audiences, despite the documented volumes of content and automated social media accounts, indicates that these malign influence networks are very unlikely to affect the election itself at this time. Similar to influence activities observed targeting the 2024 French elections, these influence networks are attempting to exploit political divisions to increase polarization; however, they themselves are not directly responsible for causing organic and legitimate political differences and disputes. Misattributing or overstating their impact could inadvertently validate the effectiveness of these operations, leading to what is often referred to as “perception hacking”, where the perceived influence of these operations is exaggerated beyond their actual impact.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com