Public Service Announcement

FBI & CISA

Alert Number: I-081424-PSA
October 18, 2024
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

---

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are issuing this announcement to raise awareness of the efforts posed by foreign threat actors to spread disinformation in the lead up to, and likely in the days following, the 2024 U.S. general election. Foreign threat actors are knowingly disseminating false claims and narratives that seek to undermine the American people's confidence in the security and legitimacy of the election process.

The FBI and CISA have no information suggesting malicious cyber activity against U.S. election infrastructure has compromised the integrity of voter registration information, prevented an eligible voter from casting a ballot, impacted the integrity of any ballots cast, or disrupted the ability to count votes or transmit unofficial election results in a timely manner. However, foreign adversaries may use false or misleading narratives that indicate otherwise to further their objectives of undermining American public confidence in democratic processes and institutions.

While foreign malign influence operations and disinformation targeting American elections are not new, the proliferation of generative artificial intelligence (AI)-enabled tools is exacerbating pre-existing tactics. Generative AI-enabled tools have lowered the barrier for foreign malicious actors to conduct more sophisticated influence campaigns. We are seeing foreign actors use these tools to develop and distribute more compelling synthetic media messaging campaigns and inauthentic news articles, as well as synthetic pictures and deepfakes (video and audio) at greater speed and scale across numerous US- and foreign-based platforms. These efforts to develop content are designed to undermine voter confidence and to entice unwitting consumers of the information to discuss, share, and amplify the spread of false or misleading narratives.

Foreign threat actors use a variety of methods, often in tandem, to knowingly spread and amplify false or misleading claims about voting processes and results, including false claims that the processes or results have been compromised by malicious cyber activity to cast doubt on the legitimacy or outcome of the vote. These actors use commercial firms, paid influence, witting and unwitting Americans, publicly available and dark web media channels, online journals, messaging applications, spoofed websites, emails, text messages, and fake online personas on U.S. and foreign platforms to spread and amplify these false claims.

In previous public service announcements, the FBI and CISA raised awareness about tactics that could be used in foreign malign influence operations to undermine public confidence in elections. Those announcements highlighted foreign threat actors' use of publicly available voter registration information as "evidence" to falsely claim that a cyber operation compromised voting systems or altered election results. Similarly, foreign threat actors may falsely claim that ransomware or distributed denial of service incidents impacting election offices could impact the security or accuracy of vote casting or counting processes.

Russian Influence Efforts

As part of efforts to combat foreign actors who are seeking to interfere in and influence U.S. elections, the Department of Justice (DOJ), in collaboration with federal partners, has taken a series of actions to degrade Russian threat actors' capabilities to conduct these malign influence campaigns.

In July 2024, the DOJ, in coordination with U.S. and international partners, exposed a covert Russian government-operated, AI-enhanced social media bot farm using specialized software to create fictitious social media personas at scale. In September 2024, the DOJ took steps to disrupt Russian government-directed foreign malign influence campaigns by seizing more than 32 internet domains controlled by Russian government malign influence actors. The DOJ also indicted employees of a Russian state-controlled media outlet who covertly funded and directed a U.S.-based company that deployed nearly $10 million to disseminate pro-Russian narratives to a U.S. audience.

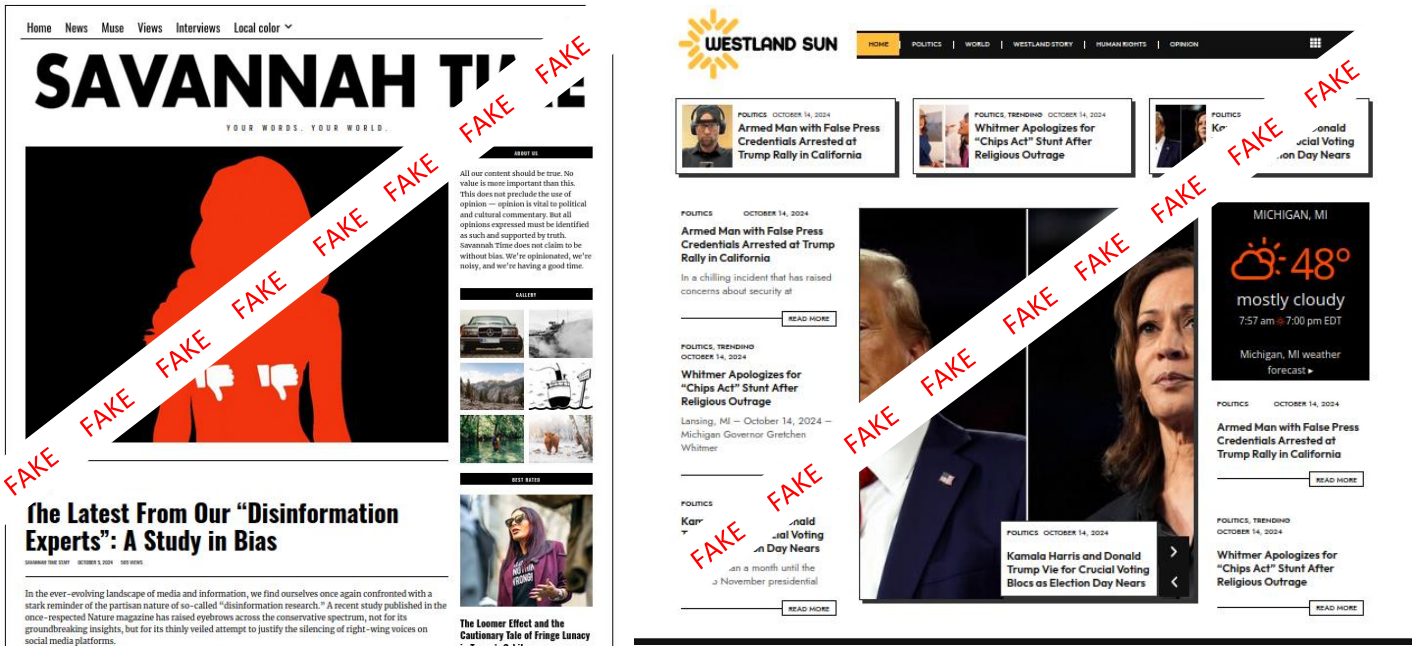
Over the course of these actions, the DOJ seized website domains that Russian malign influence actors created and deliberately designed to look like legitimate mainstream news websites (see below for examples). Many of the seized domains employed "cybersquatting,"— a method of registering a domain intended to mimic another person's or company's domain. The images below are screen captures of articles produced by these Russian government actors. These examples include websites such as "washingtonpost.pm", and "fox-news.in," which are not the real websites of the *Washington Post* and *Fox News*.

Russian government or proxy-created fake media websites falsely presenting as prominent U.S. news outlets with propaganda messaging and articles to further the threat actors' intended messaging and goals.

Russian malign influence actors also created fake social media profiles posing as U.S. citizens to direct users to these fake news websites and purchased social media advertisements to drive traffic to the specific fake articles on the fake news site. The Appendix at the end of this document provides a compilation of websites that the FBI, Department of State, or Department of Treasury have previously publicly attributed to Russian malign influence actors, as well as websites and social media accounts that the Intelligence Community has attributed to Russian malign influence actors.

Iranian Influence Efforts

In addition to Russia, Iran is also undertaking influence operations as it has in past election cycles, including through its cyber apparatus, targeting current and former U.S. government officials, members of the media, nongovernmental organizations, and individuals associated with U.S. political campaigns. Iran is probably using generative AI and inauthentic personas to hide its hand and attempt to sow discord during the 2024 U.S. election cycle. On September 27, 2024, the DOJ charged three Iranian nationals identified as employees of the Islamic Revolutionary Guard Corps (IRGC), for a wide-ranging hacking conspiracy targeting current and former U.S. officials. The three IRGC employees are alleged to have conspired to hack into accounts of current and former U.S. officials, members of the media, nongovernmental organizations, and individuals associated with U.S. political campaigns. That indictment further alleged that in June 2024, the IRGC conspirators engaged in a "hack-and-leak" operation, in which they sought to weaponize campaign material stolen from a U.S. Presidential campaign. Additionally, the FBI, U.S. Cyber Command, the Department of Treasury, and the United Kingdom's National Cyber Security Centre have previously disseminated a Joint Cybersecurity Advisory that includes a list of malicious domains used by cyber actors working on behalf of the IRGC, which is linked below. We have also seen Iranian actors use similar tactics as Russian malign influence actors where they create inauthentic news sites posing as a legitimate media organization (see example below).



Iranian government or proxy-created website presenting as a fake local news organization, which uses propaganda messaging and articles to further Iran's intended messaging and goals.

Recommendations

We urge the American public to critically evaluate the sources of the information they consume and to seek out reliable and verified information from trusted sources, such as state and local election officials. Specifically, we recommend the American public take the following precautions:

- Educate yourself and others on the tactics of foreign malign influence operations, including the use of generative AI and deep-fakes, and their goal to undermine American public confidence in U.S. democratic institutions and processes. Greater public awareness may help limit the spread of foreign malign influence campaigns.
- Seek out information from trusted, official sources, such as state and local election officials, and verify reported claims through trusted, official sources before sharing such information.
- To better understand what you are viewing, know the media and social media company policies and citation rules to denote or disclose content created or doctored with generative AI tools. When viewing content, consider who produced it and look for labels that may identify the content as AI-generated.
- Consider reporting information concerning suspicious or criminal activity, to include the distribution of knowingly false information regarding the time, place, or manner of elections designed to deprive individuals of their right to vote, to their local FBI field office.

Role of the FBI and CISA in Elections

The FBI and CISA coordinate closely with federal, state, and local election partners and provide services and information to safeguard U.S. voting processes and maintain the resilience of U.S. elections. The FBI, alongside DOJ prosecutors, is responsible for investigating and prosecuting election crimes, foreign malign influence operations, and malicious cyber activity targeting election infrastructure and other U.S. democratic institutions. The FBI does not investigate, collect, or maintain information on U.S. persons solely for the purpose of monitoring activities protected by the First Amendment. CISA, as the Sector Risk Management Agency for Election Infrastructure, is the federal government lead for working with critical infrastructure owners and operators, including the election infrastructure community, to ensure the security and resilience of election infrastructure from physical and cyber threats.

Victim Reporting and Additional Information

We encourage the public to report information concerning suspicious or criminal activity, to include the distribution of knowingly false information regarding the time, place, or manner of elections designed to deprive individuals of their right to vote, to their local FBI field office (www.fbi.gov/contact-us/field).

For additional assistance to include common terms and best practices, such as media literacy, please visit the following websites:

- Protected Voices | FBI
- #Protect2024 | CISA
- Foreign Malign Influence Center Newsroom | ODNI
- Risk in Focus: Generative AI and the 2024 Election Cycle | CISA
- Securing Election Infrastructure Against the Tactics of Foreign Malign Influence Operations | CISA
- Joint Cybersecurity Advisory: State Sponsored Russian Media Leverages Meliorator Software for Foreign Malign Influence Activity | FBI
- Joint Cybersecurity Advisory: Iranian Cyber Actors Targeting Personal Accounts to Support Operations | FBI

Other 2024 Election Cycle FBI and CISA PSAs

- Just So You Know: False Claims of Hacked Voter Information Likely Intended to Sow Distrust of U.S. Elections | FBI, CISA
- Just So You Know: Ransomware Disruptions During Voting Periods Will Not Impact the Security and Resilience of Vote Casting or Counting | FBI, CISA
- Just So You Know: DDoS Attacks Could Hinder Access to Election Information, Would Not Prevent Voting | FBI, CISA

Federal Government Actions to Disrupt Foreign Malign Influence Operations

- Justice Department Leads Efforts Among Federal, International, and Private Sector Partners to Disrupt Covert Russian Government-Operated Social Media Bot Farm | DOJ
- Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere | DOJ
- Two RT Employees Indicted for Covertly Funding and Directing U.S. Company that Published Thousands of Videos in Furtherance of Russian Interests | DOJ
- Three IRGC Cyber Actors Indicted for 'Hack-and-Leak' Operation Designed to Influence the 2024 U.S. Presidential Election | DOJ

ODNI Election Security Updates

- Early October 2024
- Mid-September 2024
- Early September 2024
- Late July 2024
- Early July 2024

Appendix A: Websites and Accounts Operated by Russian Malign Influence Actors

The following websites the U.S. Government either attributes to or assesses are highly likely to be operated by Russian malign influence actors. Websites denoted with an asterisk have previously publicly attributed to Russian malign influence actors by the FBI, Department of State, or Department of Treasury.

50statesoflie[.]com*
50statesoflie[.]media*
acrosstheline[.]press*
artichoc[.]io*
bild[.]work*
electionwatch[.]io*
electionwatch[.]live*
faz[.]ltd*
forward[.]pw*
fox-news[.]in*
grenzezank[.]com*
holylandherald[.]com*
honeymoney[.]info*
honeymoney[.]press*
infobrics[.]org*
lemonde[.]ltd*
leparisien[.]ltd*
levinaigre[.]net*
lexomnium[.]com*
liesofwallstreet[.]com*
liesofwallstreet[.]io*
meisterurian[.]io*
mypride[[.]]press*
oneworld[.]press*
pravda-ua[.]com*
rbk[.]media*
rrn[.]media*
rrn[.]world*
shadowwatch[.]us*
spicyconspiracy[.]info*
spicyconspiracy[.]io*
spiegel[.]agency*
sueddeutsche[.]co*
tagesspiegel[.]co*
tribunalukraine[.]info*
truthgate[.]us*
Ukrlm[.]info*
uschina[.]online*
uschina[.]press*
warfareinsider[.]us*
waronfakes[.]com*
washingtonpost[.]pm*
delfi[.]top*
afrinz[.]ru*
africanstream[.]media*
americanfront[.]info*
vip-news[.]org*
begemot[.]media*
syncreticstudies[.]com*
eramedia[.]com*
fortruss[.]blogspot[.]com*
geopolitica[.]ru*
globalresearch[.]ca*
inforos[.]ru*
anticrisis[.]cc*
webkamerton[.]ru*
katehon[.]com*
journal-neo[.]org*
novaresistencia[.]org*
odnarodyna[.]org*
onmedia[.]io*
openrevolt[.]info*
orientalreview[.]org*
thered[.]stream*
ritmeurasia[.]org*
rt[.]com*
ruptly[.]tv*
riafan[.]ru*
fznc[.]world*
strategic-culture[.]org*
unitedworldint[.]com*
tsargrad[.]tv*
bild[.]llc*
bild[.]ws*
washingtonpost[.]ltd*
usareally[.]com*
welt[.]ltd*
welt[.]ws*
welt[.]media*
spiegel[.]work*
nd-aktuell[.]net*
nd-aktuell[.]pro*
nd-aktuell[.]co*
obozrevatel[.]ltd*
milliyet[.]com[.]co*
albayan[.]me*
gulfnews[.]ltd*
faz[.]agency*
sueddeutsche[.]ltd*
sueddeutsche[.]cc*
tagesspiegel[.]ltd*
fraiesvolk[.]com*
fraiepozition[.]store*
fraiepozition[.]site*
bild[.]bz*
lefigaro[[.]]me*
70-putin-freunde[.]de*
freikorps[.]press*
jfriecorp[.]press*
sieben-fragen-putin[.]de*
tonline[.]life*
tonline[.]today*
t-onlinr[.]life*
t-onlinr[.]live*
t-onlinr[.]today*
delfi[.]today*
spiegel[.]fun*
spiegel[.]today*
winter-is-comming[.]de*
reuters[.]cfd*
reuters[.]cyou*

bild[.]vip*

socialharmony[.]de*

spiegel[.]ink*

dailymail[.]cfd*

spiegeli[.]life*

reuters[.]sbs*

dekommnt[.]live*

spiegelr[.]today*

t-onlinl[.]life*

t-onlinl[.]live*

t-onlinl[.]today*

sueddeutsche[.]life*

sueddeutsche[.]today*

sueddeutsche[.]site*

atlanta-observer[.]com

atlantabeacon[.]org

antifashist[.]com

american-freedom[.]org

civiccommentary[.]org

civiccorner[.]org

civiccreed[.]com

civiccurrent[.]com

civiccurve[.]com

conservativecamp[.]org

conservativecatch[.]org

conservativechannel[.]org

conservativecircuit[.]com

derglaube[.]online

derleitstern[.]cc

derleitstern[.]com

repubblica[.]icu*

manabalss[.]li*

sueddeutsche[.]online*

delfi[.]life*

spiegeli[.]live*

blld[.]live*

ukcommunity[.]vip*

spiegelr[.]life*

foxnews[.]cx*

inforos[.]ru*

infosco[.]org*

southfront[.]org

allons-y[.]social

brennendefrage[.]com

alternativereport[.]us

candidat[.]news

candidat_news<X account>

capitolpulse[.]org

conservativecompass[.]org

conservativecorridor[.]com

conservativecourier[.]org

cropmarketchronicles[.]cc

cropmarketchronicles[.]us

dc-free-press[.]org

deintelligenz[.]com

deintelligenz[.]io

democracydepth[.]com

democracydrive[.]org

derbayerischelowe[.]info

derglaube[.]com

repubblica[.]world*

musubalss[.]org*

dailymail[.]cam*

repubblica[.]life*

spiegeli[.]today*

itcb[.]life*

spiegelr[.]live*,

50StatesOfLie<X account>

AcrossTheLine11<X account>

alhiwar[.]cc alhiwar[.]me

bostontimes[.]org

besuchszweck[.]org

brennende_frage<X account>

brennendefrage[.]cc

carsondispatch[.]com

centernewscentral[.]com

centerpointbeacon[.]com

civiccentury[.]org

conservativecontext[.]com

democracydive[.]com

daybreakdigest[.]org

derrattenfanger[.]io

derrattenfanger[.]net

DragonflyTimes<Xaccount>

epochpost[.]org

flagstaffpost[.]com

flyoverbeacon[.]com

franceeteu[.]today

franceeteu<X account>

freedomfacade[.]com

arbeitspause[.]org
freedomfixture[.]com
freedomforge[.]info
freedomfoundry[.]info
freemediaforum[.]info
gopguardian[.]com
governancegaze[.]com
grunehummel[.]com
GruneHummel<facebookName>
hauynescherben[.]net
hauynescherben[.]press
hauynescherben<Xaccount>
heartlandharbor[.]org
heartlandhaven[.]org
heartlandheadlines[.]net
heartland-inquirer[.]org
honestcitizens[.]org
houstonpost[.]org
il_corrispondente[.]com_<instagramName>
il-corrispondente[.]com
rybar<telegramName>
corrispondente[.]io
interventionist[.]cc
interventionist[.]com
interventionist[.]us
Intrvntnst<X account>
kaputteampel[.]cc
kaputteampel[.]com
KaputteAmpel<X account>
kbsf-tv[.]com
lansingtribune[.]org
la-sante[.]info
laterrasse[.]io
laterrasse[.]online
leaderledger[.]net
lebelligerant[.]com
lebelligerant[.]io
lebelligerant<X account>
le-continent[.]com
lesfrontieres[.]media
lesfrontieres<X
southfront[.]press
lavirgule[.]news
lesifflet[.]cc
lesifflet[.]net
LexOmnium<X account>
libertylagoon[.]org
libertylantern[.]org
libertylaunch[.]org
libertylectern[.]org
libertypressnews[.]com
libertyvoice[.]info
lonestarcrier[.]com
madison-gazette[.]org
maplechronicles<telegramName>
meriblood<telegramName>
miastagebuch[.]com
nationalcrier[.]com
nationalmatters[.]org
nationalnarrative[.]org
nationnotebook[.]com
newscenterpress[.]org
news-front[.]su
strategic-culture[.]su
orientalreview[.]su
journal-neo[.]su
noticiasbravas[.]com
notrepays[.]today
observateurcontinental[.]Fr
omnam[.]life
oraclenews[.]org
partyperspective[.]com
patrioticpage[.]com
patrioticparade[.]com
patrioticpioneer[.]com
patrioticpulse[.]info
phoenixpatriot[.]org
policypaddock[.]com
policypassage[.]com
policypatch[.]com
policypath[.]org
policypeak[.]org
policyplatform[.]info
policyporch[.]org
politicalpioneer[.]com
politicalplot[.]org
politicalporch[.]com
politicostream[.]com
politnavigator[.]news
politnavigator<telegram Name>
politnavigator<X account>
politnavigator<youTube Name>
polskikompas[.]com
pulsepress[.]org
purplestatepost[.]com
raleigh-herald[.]com
Rattenfangernet<X account>
red-blue-tribune[.]com
redstategazette[.]com
redstatereport[.]net
republicrally[.]com
republicrange[.]com
republicregard[.]com
republicreview[.]net
republicripple[.]com
republicroot[.]com
republicroots[.]org
republicrundown[.]com
rightrealm[.]net
rightresonance[.]org
rightrevival[.]org
rightrundown[.]com
senatesight[.]com signaldaily[.]org
silverstatesignal[.]org

southfronteng<telegram account>

statestage[.]org

unitytrend[.]com

voice-of,europe[.]eu

votervista[.]net

TEXASvsUSA<telegramName>

TEXASvsUSA<X account>

wanderfalke[.]net

naebc[.]com

rybar_force<X account>

southfroneng<X account>

thearizonaobserver[.]com,

ULM_Info<X account>

ukraine-inc[.]info

bild[.]asia

topicdujour<telegram account>

interventionist[.]io

facts[.]matter[.]me

sueddeutsche[.]me

rightreview[.]org

SouthFrontEnThree<facebook>

tribunetimes[.]org

TruthGateOff<X account>

vanguardviews[.]com

spiegel[.]pro

dailymail[.]top

SpConspiracy<X Name>

faz[.]life

scopestory[.]com

Appendix B: Websites Operated by Iranian Malign Influence Actors

The following websites the U.S. Government either attributes to or assesses are highly likely to be operated by Iranian malign influence actors.

Evenpolitics[.]com

Savannahtime[.]com

Westlandsun[.]com

Niothinker[.]com

Afromajority[.]com

Al-saria[.]com