Report

The State(s) of Foreign Information Operations

A State-by-State Look at Foreign Information Manipulation in the United States

G | M | F Alliance for Securing Democracy

Krystyna Sikora and Bret Schafer

Introduction

It is easy to dismiss foreign information operations as playing out at the national level, designed to influence federal policymakers and Beltway insiders. But these threats transcend the "Beltway Bubble". Increasingly, foreign nation-state actors are running operations that exploit trust in local sources and impact state and local communities.

US adversaries like Russia, China, and Iran are refining their information tools and tactics to better target individuals and exacerbate divisions within the United States to destabilize the country at home and weaken it on the world stage. These nation states are increasingly exploiting domestic actors to launder and manipulate content that originates in Moscow, Beijing, and Tehran and ultimately reaches American audiences who have no way of knowing they are on the receiving end of foreign information operations. They are also experimenting with generative artificial intelligence (AI), which, according to the US intelligence community, has allowed nation-state actors to "improve and accelerate" their operations, potentially enabling them to reach more Americans with more targeted content.

Adversaries understand that state and local governments and communities are foundational to the strength of American democracy, so it is no surprise that they have targeted individuals and issues at the local level. In some cases, adversarial nations seek favorable outcomes around local policy issues; in others, they use local debates as Trojan horses to advance their broader geopolitical agendas. In others still, they attempt to influence views on the integrity of US elections and institutions or disenfranchise American citizens in specific communities to destabilize and erode trust in American democracy. But in all cases, American democratic discourse and the country's information space—messy as they can sometimes be—are being used as primary vectors to advance foreign interests. If Americans lack that understanding, their communities—and the country—are left vulnerable.

This report outlines an example of a foreign information operation targeting each of the 50 US states and the District of Columbia. Each case study indicates the foreign threat actor (if known) and explains the tools, tactics, and motivations for targeting Americans at the state and local level.

Methodology and Key Findings

The report uses the DISARM Red framework to categorize the perceived objectives of, and known tactics, techniques, and channels used by, the threat actors identified in each case study. This coding process helps to identify commonalities across information operations playing out at the state and local level, allowing for a more complete understanding of the threat landscape. At the same time, our decision to highlight only one case per state meant that there was an element of subjectivity in the selection process, especially in states that are more regularly targeted by foreign actors, such as swing states. In states where there were multiple documented cases of foreign information manipulation, we typically chose a case that allowed us to highlight the wide diversity of threat actor tactics and techniques used to target American audiences. Had we applied a different selection criterion—for example, cases that had the largest perceived impact—we could have, and likely would have, selected different cases for some states. The following analysis should therefore be viewed as an effort to provide additional context, rather than a methodologically rigorous assessment of the most common threat actors, objectives, and methods used in state and local information operations. That caveat aside, we found that:

- Russia (26 cases) was the most common threat actor in the cases we examined, followed by China (14 cases), multiple countries (4 cases), unknown (3 cases), Iran (2 cases), and other countries (2 cases).

- In the cases we examined where Russia was the threat actor, the most common objective, by far, was to polarize and divide the American public. In cases where China was the threat actor, the most common objective was to cultivate support for Chinese state interests.

- Although social media platforms were the most common channel (34 cases) for conducting information operations at the state and local level, traditional media outlets were used in 12 cases, while inauthentic news sites were used as assets in eight cases. This demonstrates that information operations do not just exploit social media platforms but the entire information ecosystem.

- In total, we documented more than 20 different tactics and techniques, from the cultivation of ignorant agents to the outsourcing of operations to external organizations, used by foreign threat actors to establish assets and legitimacy in state and local information operations.

From Alabama to Wyoming: State examples of foreign information manipulation

Chinese influence operation targets down-ballot races, including in Alabama

State: Alabama

Threat Actor: China

Date: 2024

Objectives: Undermine (smear opponents)

Select Channels & Affordances: Social Media Platforms

Tactics & Techniques: Develop Narratives (leverage existing narratives); Develop Content (text-based); Establish Assets (pre-existing assets); Deliver Content (direct posting and comment or reply on content); Microtarget (create localized content); Maximize Exposure (utilize Spamouflage)

In the months leading up to the 2024 presidential election, the Chinese state-linked influence network known as "Spamouflage" targeted Republican Representative Barry Moore of Alabama and other congressional candidates to sway down-ballot races. According to Microsoft, which identified the influence campaign, the operation employed dozens of inauthentic accounts to post negative content about candidates who had publicly denounced the Chinese government and its policies. The accounts often accused the candidates of corruption or promoted opposition candidates. The Microsoft report notes the network specifically criticized Moore's support for Israel, frequently using antisemitic language. The posts about Moore received engagement from legitimate online users, which bot accounts in the network subsequently amplified. Other targeted members of Congress in this operation included Tennessee Senator Marsha Blackburn, Florida Senator Marco Rubio, and Texas Representative Michael McCaul.

Kremlin actors create and amplify petition for Alaska's secession and return to Russia

State: Alaska

Threat Actor: Russia

Date: March 2014

Objectives: Cultivate Support (cultivate support for an initiative) and Distract

Select Channels & Affordances: Online Polls, Community Forum Platforms, Social Media Platforms

Tactics & Techniques: Develop Narratives (develop new narratives); Develop Content (text-based and video-based content); Establish Assets (newly created asset); Establish Legitimacy (impersonated persona); Maximize Exposure (bots amplify via automated forwarding and reposting and inauthentic sites amplify news and narratives); Persist in the Information Environment (continue to amplify)

In March 2014, in the very early stages of Russia's online operations targeting the 2016 US presidential election, a pro-Kremlin Russian outfit created a petition on the official White House website for Alaska's secession from the United States and its return to Russia, which automated Russian bots subsequently amplified across various social media platforms. The petition—written using clumsy English, likely with an automated translation tool—generated over 39,000 online signatures within days, more than a third of the 100,000 signatures needed for a formal government response. Many of the signatures were likely generated using automated bots. Russian-linked accounts continue to entertain this narrative. More recently, a network of Georgian and Russian-language Facebook accounts and websites disseminated a fabricated English-language video that falsely appeared to be published by the legitimate US news outlet "Alaska Public Media"—even displaying the outlet's logo—which claimed that Alaska was holding a referendum to join Russia on November 4, 2022.

Chinese firm leverages newswire service to place propaganda articles in Arizona outlet

State: Arizona

Threat Actor: China

Date: 2023

Objective: Facilitate State Propaganda, Cultivate Support (boost reputation), and Undermine (smear opponents)

Select Channels & Affordances: Traditional Media (newspaper)

Tactics & Techniques: Develop Content (re-use existing content and deceptively labelled content); Establish Legitimacy (co-opt trusted sources); Deliver Content (text-based); Persist in the Information Environment (launder information assets)

The Chinese private company Shanghai Haixun Technology used a newswire service to place pro-Beijing articles on the websites of legitimate American news outlets, including the Arizona Republic, according to an investigation by the cybersecurity firm Mandiant. The pieces—which appeared in at least 32 news outlets—tried to portray the United States negatively and highlight China's successes. Article topics included criticism of then-Speaker of the House of Representatives Nancy Pelosi's visit to Taiwan, as well as US policy on fentanyl, human rights, and race. The articles were often directly reproduced from Chinese state media or state-funded think tanks. Haixun placed the articles using a newswire distribution service called CloudQuote.io, which is run by the California-based firm FinancialContent. The firm also allegedly used the freelance service Fiverr to hire people to promote content that aligns with China's political narratives and to share links to published articles. The Arizona Republic began redirecting visitors of the pages where Haixun content appeared to other pages on its website after a reporter contacted the news outlet.

Faux local Arkansas news outlet republishes RT articles, attributes them to fictitious author

State: Arkansas

Threat Actor: Unknown

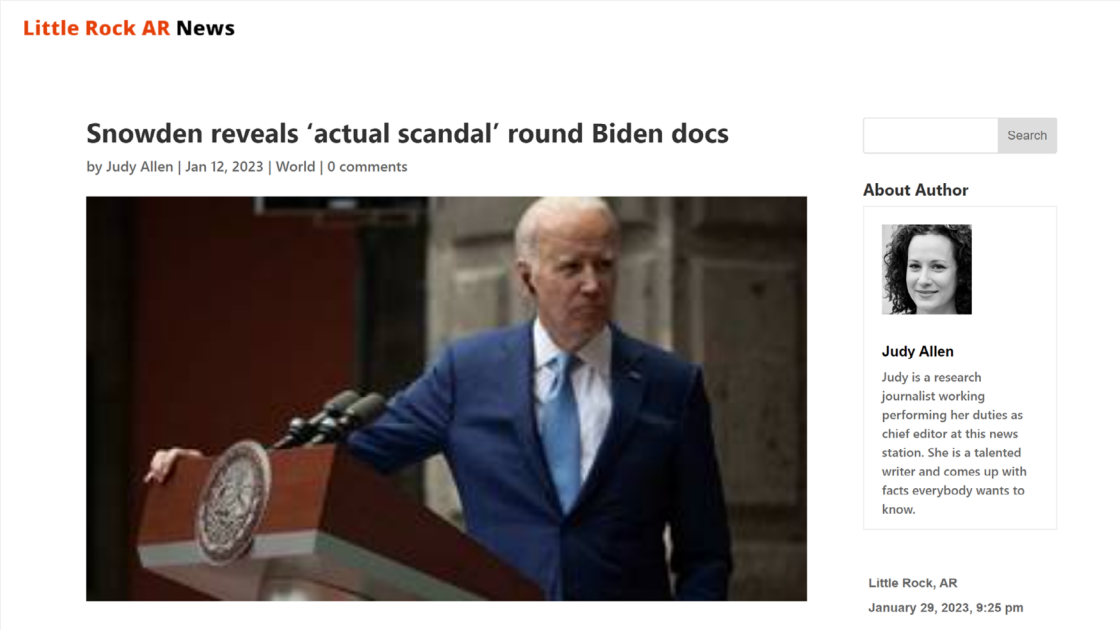
Date: 2022-2023

Objective: Make Money (generate ad revenue) and Facilitate State Propaganda

Select Channels & Affordances: Website Assets

Tactics & Techniques: Develop Content (appropriate content); Establish Assets (develop owned media assets); Establish Legitimacy (create inauthentic news site, AI-generated account imagery, and journalist persona); Maximize Exposure (bypass content blocking); Persist in the Information Environment (launder information assets)

A website posing as a local Arkansas news site routinely sourced stories from the Russian state-controlled media organization RT and attributed them to fictitious journalists, according to an ASD research investigation. The faux outlet littlerockarnews.com, which is now defunct, presented itself as a local site focused on news relevant to Little Rock, Arkansas. But mixed in with coverage of local politics and sports—presumably sourced from genuine local news outlets—were "world news" stories sourced from RT. In at least one case observed by ASD, an RT article published on the website was attributed to an almost certainly fictitious author named "Judy Allen" who routinely churned out dozens of articles per day. The author's profile photo did not produce any matches in a reverse image search and was likely generated by AI, helping to mask the true source of the information "she" produced.



A screenshot of a laundered RT article on Little Rock AR News "written" by the fictitious Judy Allen.

Faux San Francisco news outlet publishes fake content to undermine presidential candidate

State: California

Threat Actor: Russia

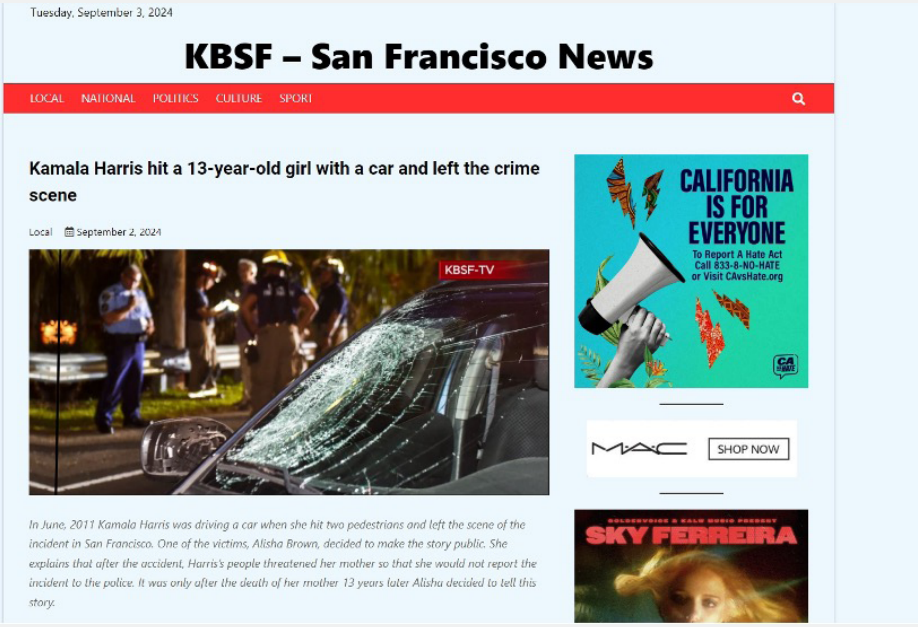
Date: 2024

Objective: Undermine (smear opponent)

Select Channels & Affordances: Website Assets

Tactics & Techniques: Develop Narratives (develop new narratives); Develop Content (create fake research and deceptively edit video and images); Establish Legitimacy (create inauthentic news site and fabricated persona); Conduct Pump Priming (seed distortions); Deliver Content (post content); Persist in the Information Environment (launder information assets and delete account activity)

In the months leading up to the 2024 presidential election, the Russian-linked influence network known as Storm-1516 created a website posing as a fictitious San Francisco local news outlet to publish fake content to denigrate Vice President (and former California Senator) Kamala Harris' campaign. In September 2024, the faux news website KBSF-TV published an article that falsely claimed that Harris was involved in a 2011 hit-and-run accident in San Francisco that left a 13-year-old girl paralyzed. The article included an embedded video that featured a Russian paid actor reciting the incident from a wheelchair, as well as x-ray scans purporting to be from the accident but were taken from published medical articles. The faux news website was created in late August and went offline days after it published the story on September 2. The video generated millions of views, according to Microsoft.



A screenshot of the faux local San Francisco site KBSF-TV showing a fabricated news article aimed at denigrating Harris' campaign.

Russian hacking group poses as Islamic State group to intimidate US military spouses, including Colorado woman

State: Colorado

Threat Actor: Russia

Date: 2015

Objective: Cause Harm (intimidate), Degrade Adversary, and Dismay

Select Channels & Affordances: Direct Messaging and Social Media Platforms

Tactics & Techniques: Develop Content (create new hashtags and text-based content); Establish Assets (compromised asset); Establish Legitimacy (impersonated persona); Deliver Content (direct posting); Drive Online Harms (harass); Persist in the Information Environment (misattribute activity)

In 2015, the Russian hacking group known as Fancy Bear posed as Islamic State group (IS) supporters and hacked into the US military's Central Command Twitter account. A few weeks later, the hacking group sent online threats to five spouses of US military personnel, who were members of the advocacy group Military Spouses of Strength. All five spouses, including a Colorado resident named Angela Ricketts, had spoken out against the Central Command hacking in a CNN article. In the original Central Command Twitter hack, Fancy Bear replaced the account's profile and cover photo with IS insignia and posted a series of tweets that purported to reveal classified information, expressed sympathy for IS, and threatened military personnel. The hackers claimed to be a group called "CyberCaliphate". Following the publication of the CNN article, Fancy Bear again posed as "CyberCaliphate" and breached the Military Spouses of Strength's Twitter account and posted pro-IS messages and public threats. Five of the group's members were also directly contacted. Ricketts received messages that threatened her family members and alleged that IS had breached her computer.

Israel commissions covert influence campaign to target US lawmakers, including Connecticut Senator

State: Connecticut

Threat Actor: Israel

Date: October 2023 – Present

Objective: Cultivate Support (cultivate support for an initiative), Distract, and Degrade Adversary

Select Channels & Affordances: Social Media Platforms

Tactics & Techniques: Develop Narratives (leverage existing narratives and integrate target audience vulnerabilities into narratives); Establish Assets (outsource content creation to external organization, bulk assets, and AI-generated account imagery); Establish Legitimacy (create inauthentic news sites and fabricated personas); Deliver Content (post inauthentic social media comments); Maximize Exposure (trolls amplify and manipulate); Persist in the Information Environment (distance reputable individuals from operation)

In October 2023, Israel's Ministry of Diaspora Affairs organized and paid for a covert online influence campaign targeting at least 128 members of Congress—including Democratic Senator Richard Blumenthal of Connecticut—with pro-Israel content amid the war in Gaza. According to a New York Times investigation, the Israeli ministry paid Stoic, a Tel Aviv-based marketing firm, $2 million to carry out the campaign. Stoic created approximately 600 fake social media accounts posing as Americans across multiple platforms including X, Facebook, and Instagram. These accounts posted more than 2,000 coordinated comments per week that supported Israel's military actions, slamming Palestinian rights groups, and dismissing claims of human rights abuses. The accounts also targeted US—and particularly Black and Democratic—lawmakers with online posts urging them to continue funding Israel's military. Blumenthal was reportedly targeted 88 times. The operation also created three faux English-language news sites that featured pro-Israel articles and reportedly used OpenAI's tools to generate posts and profile pictures. Meta also announced it had removed more than 500 Facebook accounts, 11 pages, and one group, as well as 32 Instagram accounts linked to the network.

Russia-linked news company registers as Delaware LLC to conceal foreign roots

State: Delaware

Threat Actor: Russia

Date: 2019

Objective: Undermine (polarize)

Select Channels & Affordances: Website Assets, Social Media Platforms, and Video Platforms

Tactics & Techniques: Develop Narratives (leverage existing narratives); Develop Content (video-based content); Establish Assets (develop owned media assets; Establish Legitimacy (co-opt influencers); Maximize Exposure (post across platforms); Conceal Infrastructure (conceal sponsorship)

After Facebook announced a new policy to label foreign state-controlled media, news programs run by Maffick Media—a German company whose majority stakeholder was Ruptly, a subsidiary of Russian state media organization RT—reincorporated as a Delaware-based company called Maffick LLC. The new Delaware-based company is now entirely owned by former RT journalist Anissa Naouai, who was previously a minority owner of the German entity with 49% of the shares. Maffick's news programs were designed to appeal to millennial, digitally inclined, English-speaking audiences and often take stances that align with the Russian government's. Maffick's most viewed program "In the NOW"—a former RT program that was also hosted by Naouai and specialized in creating short, shareable news content that blended in Russian propaganda—had 4.8 million Facebook followers. Following the reincorporation, Maffick LLC sued Facebook for labeling "In the NOW" and its companion channels as Russian state-controlled media. Facebook previously suspended three pages associated with Maffick Media channels—Soapbox, Backthen, and Waste-Ed—that accumulated more than 30 million video views. The case was dismissed in 2021.

Chinese firm organizes and amplifies DC protests

State: District of Columbia

Threat Actor: China

Date: 2022

Objective: Motivate to Act (encourage) and Cultivate Support (cultivate support for an initiative)

Select Channels & Affordances: Social Media Platforms and Traditional Media (newspaper)

Tactics & Techniques: Establish Assets (cultivate ignorant agents); Establish Legitimacy (co-opt influencers); Drive Offline Activity (organize events and pay for physical action); Maximize Exposure (incentivize sharing); Persist in the Information Environment (conceal sponsorship)

The Chinese marketing firm Shanghai Haixun Technology commissioned and promoted at least two protests in Washington, DC that took place in June and September 2022, respectively, according to an investigation by Mandiant. The first protest allegedly was in response to the 2022 International Religious Freedom (IRF) Summit, an annual event held in DC that aims to bring awareness to restrictions on religious freedom. The second was allegedly organized in response to a June 2022 US government decision to ban all goods produced in Xinjiang, a region that has drawn controversy over allegations of human rights abuses against Uyghurs. Huaxin reportedly hired a 24-year-old Baltimore musician and entrepreneur, Imani Wj Wright, to organize one of the protests using the online freelance service platform Upwork. The job posting listed for $1,500 and sought a "United States journalist" to report on the IRF Summit and conduct interviews with "novel and sharp questions". After Wright agreed, the client asked him to also stage a protest. Wright did not know that the client had links to pro-China operatives. Although both protests drew minimal crowds, Huaxin amplified their coverage, including by publishing a press release about the protests that was then distributed to legitimate American news outlets via a newswire service and employing bot accounts to post about the events. In at least one instance, Huaxin also used the freelance service Fiverr to pay an unwitting American to share a video of the protest for $10.

Iranian hackers send email threats posing as extremist group to Florida voters

State: Florida

Threat Actor: Iran

Date: October 21, 2020

Objective: Cause Harm (intimidate), Dissuade from Acting (deter), and Undermine (polarize and smear)

Select Channels & Affordances: Email Platform and Direct Messaging

Tactics & Techniques: Develop Narratives (integrate target audience vulnerabilities into narrative); Develop Content (obtain private documents and text-based content); Establish Assets (email domain asset); Establish Legitimacy (impersonated personas); Persist in the Information Environment (misattribute activity)

Two weeks before Election Day in 2020, two Iranian hackers sent threatening messages that purported to be from an extremist group to thousands of voters in several states, including Florida. According to a US Department of Justice (DOJ) indictment, the hackers attempted to compromise at least 11 state voter websites and successfully obtained confidential voter information concerning more than 100,000 voters from at least one state election website. They subsequently used this information to send intimidating emails to registered Democrats claiming to be the Proud Boys—a designated extremist group with ties to white nationalism—that threatened recipients with physical injury if they did not change their party affiliation and vote for President Donald Trump. The emails came from the faux email address info@officialproudboys[.]com. The same hackers also posed as Proud Boys members to send emails and Facebook messages to Republican members of Congress and individuals associated with Trump's campaign that falsely alleged Democratic Party planned to conduct election fraud.

Russia fabricates and amplifies video depicting voter fraud in Georgia

State: Georgia

Threat Actor: Russia

Date: October 2024

Objectives: Divide and Undermine (polarize)

Select Channels & Affordances: Video Platforms and Social Media Platforms

Tactics & Techniques: Develop Narratives (develop new narratives and leverage existing narratives); Develop Content (deceptively edit video); Establish Assets (cultivate ignorant agents); Establish Legitimacy (fabricated personas); Conduct Pump Priming (seed distortions); Maximize Exposure (incentivize sharing); Persist in the Information Environment (conceal sponsorship)

Days before the 2024 presidential election, Russian state-linked actors manufactured and amplified a video that purported to show voter fraud in Georgia. The video falsely depicted two Haitian immigrants who claimed they would illegally vote at least twice in Georgia—once in Gwinnett County and again in Fulton County—for Harris. Although the video was quickly debunked by Georgia Secretary of State Brad Raffensperger, it garnered millions of views on X. In a joint statement, the Office of the Director of National Intelligence (ODNI), the Federal Bureau of Investigation (FBI), and the Cybersecurity and Infrastructure Security Agency (CISA) claimed the video was part of Russia's broader strategy to undermine trust in the election and stoke divisions. A CNN investigation later revealed that Simeon Boikov—a registered Russian agent based in Australia who works for Russian state media and has played a role in past influence campaigns—paid an unwitting conservative social media influencer in Massachusetts $100 to post the video. The influencer admitted this was not the first time Boikov had paid him to post content.

Chinese operatives use AI to spread conspiratorial narratives about Hawaii wildfires

State: Hawaii

Threat Actor: China

Date: August 2023

Objective: Divide and Undermine (polarize)

Select Channels & Affordances: Social Media Platforms and Microblogging Platform

Tactics & Techniques: Develop Narratives (leverage existing conspiracy theory narratives); Develop Content (develop AI-generated images); Establish Assets (bulk created assets); Deliver Content (direct posting); Maximize Exposure (post across platform and utilize Spamouflage); Persist in the Information Environment (play the long game)

In August 2023, the Chinese state-linked network Spamouflage exploited the deadly wildfires in Maui to spread conspiratorial narratives and test new influence tactics, including disseminating AI-generated images. The campaign—which comprised a network of at least 85 fake social media accounts and blog posts across dozens of websites and platforms—alleged that the US government had deliberately started the fires to test a military-grade "weather weapon". These posts were often accompanied by sensational AI-generated images of burning coastal roads and residences to presumably to drive engagement. Microsoft's Threat Analysis Center, which discovered the campaign, identified inauthentic posts in 31 languages and suggested the purpose of the campaign was to build the network's audience and find new authentic accounts it could engage with for future influence operations.

Russian operatives used Facebook to organize anti-immigrant protest in Idaho

State: Idaho

Threat Actor: Russia

Date: August 2016

Objective: Cause Harm (spread hate), Divide, and Undermine (polarize)

Select Channels & Affordances: Social Media Platforms and Online Community Page

Tactics & Techniques: Develop Narratives (leverage existing narratives and conspiracy narratives); Establish Assets (newly created assets and create community or subgroup); Conduct Pump Priming (seed distortions); Deliver Content (direct posting); Maximize Exposure (amplify existing narrative); Drive Offline Activity (organize events)

In the months leading up to the 2016 presidential election, operatives linked to Russia's Internet Research Agency (IRA) used Facebook's event management tool to remotely organize protests across the country, including an anti-immigrant demonstration in Twin Falls, Idaho in August. The Facebook event, called "Citizens before refugees", was created by the IRA-operated Facebook page "Secured Borders" that had more than 133,000 followers and regularly posted xenophobic messages and praised then-candidate Trump's tough line on immigration. The Facebook event fed off a series of misleading reporting and incendiary claims that had emerged online earlier that year linking Muslim immigrants to crime in Twin Falls. Forty-eight people clicked that they were interested in attending the event.

Russian-controlled website impersonating Chicago news outlet publishes Kremlin propaganda

State: Illinois

Threat Actor: Russia

Date: 2024

Objective: Degrade Adversary, Divide, and Undermine (polarize and smear)

Select Channels & Affordances: Website Assets, Social Media Platform, Traditional Media

Tactics & Techniques: Develop Narratives (develop original conspiracy theory narrative); Develop Content (inauthentic news sites, deceptively edited video content, and AI-generated text); Establish Legitimacy (create inauthentic news site and fabricated personas); Deliver Content (direct posting); Maximize Exposure (bots amplify by reposting and forwarding and inauthentic news sites amplify news and narratives); Persist in the Information Environment (launder information assets)

A Russian state-sponsored operative created a network of at least 167 Russian-linked websites that mimicked local news outlets in the United States—including one masquerading as an Illinois newspaper called the "Chicago Chronicle"—to influence Americans ahead of the 2024 presidential election. The network of faux news sites published stories that aligned with the Kremlin's interests, often with the intent to polarize or deceive American audiences. According to an investigation by NewsGuard, which identified the network, the faux Chicago news site published an article that falsely claimed that Pfizer vaccine trials authorized by Ukrainian President Volodymyr Zelenskyy resulted in the deaths of over 40 Ukrainian children. The article included an embedded fabricated YouTube video which purported to show a Pfizer whistleblower named "Anna Sakhno" discussing the supposed clinical trials. The story was amplified by pro-Kremlin bots and later picked up by Russian state media, which cited the Chicago Chronicle as a reputable American publication. AI software was used to write fabricated articles or rewrite legitimate news stories with fake elements on faux news websites across the network.

Network of faux local news sites comprising fake Indiana outlet launders Russian and Chinese state media

State: Indiana

Threat Actor: Unknown

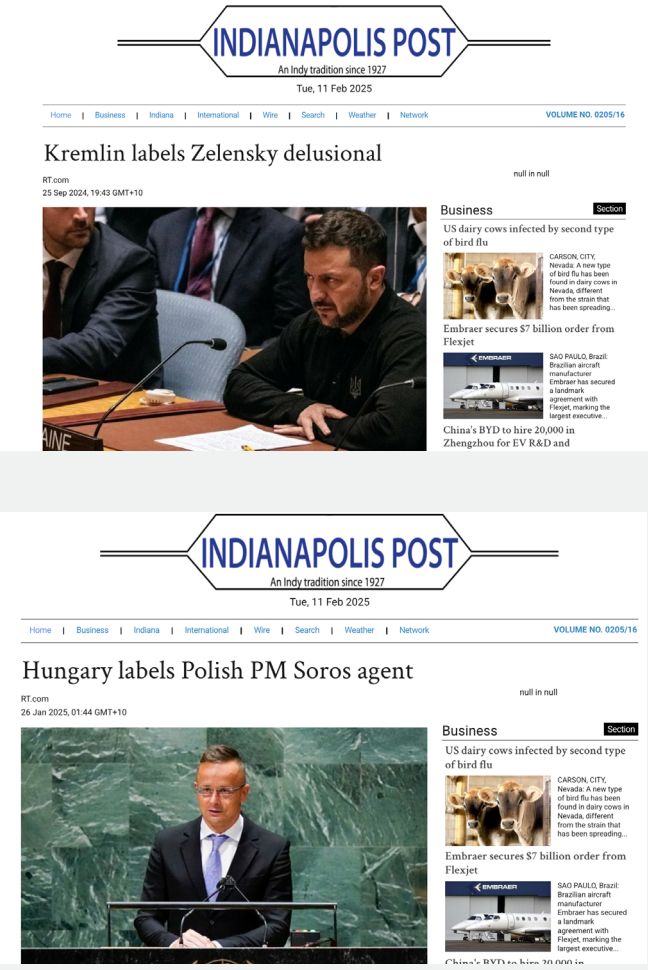
Date: 2000 - Present

Objective: Make Money (generate ad revenue) and Facilitate State Propaganda

Select Channels & Affordances: Website Assets

Tactics & Techniques: Re-use existing content (appropriate content); Establish Legitimacy (create inauthentic news site and journalist personas); Manipulate Platform Algorithms (bypass content blocking); Persist in the Information Environment (launder information assets)

A network of faux news outlets—including one called the Indianapolis Post—routinely sources propaganda content from Russian and Chinese state-controlled media. The Indianapolis Post presents itself as a local Indiana outlet, claiming to be an "Indy tradition since 1927" and featuring articles about local Indiana news. However, the international section of the site often outsources articles from Russian state-controlled media outlet RT and Chinese state-run Xinhua that are intended to divide or shape Americans' opinions. For example, the Indianapolis Post has published RT content that claims Ukrainian President Volodymyr Zelenskyy is "delusional" and alleges the Polish Prime Minister is an agent of philanthropist George Soros. The Indianapolis Post is a part of the Big News Network, an incorporated news agency based in Dubai with offices in Australia that operates more than 500 websites across the globe that present themselves as local, regional, or national news outlets. The Big News Network reposts content from a variety of news sources—sometimes with attribution and sometimes without—but the network has routinely surfaced in ASD research as a primary propagator of Russian and Chinese state media content.



Examples of an RT articles reposted on Indianapolis Post.

Russian operatives purchase ad amplifying election rigging claims in 2016 Iowa Caucus

State: Iowa

Threat Actor: Russia

Date: February 2020

Objective: Divide and Undermine (polarize and smear)

Select Channels & Affordances: Social Media Platforms

Tactics & Techniques: Develop Narratives (leverage existing narratives); Develop Content (develop text-based content and memes); Establish Assets (newly created assets and create community or subgroup); Establish Legitimacy (fabricated and social cause personas); Conduct Pump Priming (seed distortions); Deliver Content (direct posting and deliver ads); Maximize Exposure (bots amplify via automated forwarding and reposting and trolls amplify and manipulate)

In the months leading up to the 2016 presidential election, Russia's Internet Research Agency (IRA) amplified claims that a presidential candidate committed voter fraud during the Iowa Democratic caucus. According to a 2018 indictment by the DOJ, accounts linked to the IRA began purchasing advertisements to promote a post made on its Facebook account "Stop A.I." (Stop All Invaders/Stop All Immigrants) which alleged that "Hillary Clinton has already committed voter fraud during the Democrat Iowa Caucus". The IRA operation seized on the intraparty division and domestic narratives that emerged following close caucus results between Clinton and her opponent, Bernie Sanders, in which Clinton won with 49.8% of state delegates to Sanders' 49.6%.

Russian operatives purchase Facebook advertisement promoting LGBTQ+ protest in Kansas

State: Kansas

Threat Actor: Russia

Date: 2016

Objective: Cause Harm (spread hate), Divide, and Undermine (polarize)

Select Channels & Affordances: Social Media Platforms

Tactics & Techniques: Develop Narratives (leverage existing narratives); Develop Content (develop memes); Establish Assets (create community or subgroup); Establish Legitimacy (activist personas); Microtarget (purchase targeted advertisements and create localized content); Deliver Content (share memes); Drive Offline Activity (organize events)

In the months leading up to the 2016 presidential election, Russia's Internet Research Agency (IRA) purchased more than 3,500 Facebook advertisements to stoke division, including one promoting a counterprotest against the Westboro Baptist Church—a Christian denomination known for its inflammatory anti-gay rhetoric—in Lawrence, Kansas on May 25. The advertisement was directed toward LGBTQ+ audiences and was purchased and amplified by the Facebook group "LGBT United", an IRA-run account that regularly posted memes and content on LGBTQ+ matters.

Chinese-state operatives spread false information about train derailment in Rockcastle County, Kentucky

State: Kentucky

Threat Actor: China

Date: November 2023

Objective: Divide and Undermine (polarize)

Select Channels & Affordances: Social Media Platforms and Microblogging Platform

Tactics & Techniques: Develop Narratives (leverage existing narratives, develop original conspiracy narratives, and respond to breaking news event); Develop Content (text-based); Establish Assets (pre-existing asset); Deliver Content (direct posting); Maximize Exposure (utilize Spamouflage)

On November 22, 2023, a train carrying molten sulfur derailed and leaked its contents in Rockcastle County, Kentucky. The Chinese state-linked influence network known as Spamouflage subsequently exploited the derailment to spread false information with the intent to heighten political division and denigrate trust in the US government. The campaign falsely insinuated that the government was responsible for the Kentucky derailment—and other recent derailments, including a train disaster in East Palestine, Ohio that was similarly exploited by a Russian influence campaign—and suggested that the government is "deliberately hiding something". Some posts even tied the derailment to a string of unfounded theories that the US government is supposedly involved in national tragedies such as the attacks of September 11, 2001 and the assault on Pearl Harbor. Other posts falsely claimed that the government prohibited reporters and journalists from investigating the derailment, stifling free speech.

Russian-linked troll factory orchestrates online hoax about chemical explosion in Louisiana

State: Louisiana

Threat Actor: Russia

Date: September 11, 2014

Objective: Degrade Adversary and Dismay

Select Channels & Affordances: Social Media Platforms and Website Assets

Tactics & Techniques: Develop Narratives (develop original conspiracy theory narratives); Develop Content (create inauthentic news articles and deceptively edit images and video); Establish Assets (establish newly created assets); Establish Legitimacy (inauthentic news site and local personas); Microtarget (create clickbait and localized content); Conduct Pump Priming (seed distortions and trial content); Deliver Content (direct posting); Maximize Exposure (bots amplify via automated forwarding and reposting; trolls amplify and distort; inauthentic sites amplify); Persist in the Information Environment (misattribute activity)

In 2014, Russia's Internet Research Agency (IRA) orchestrated an elaborate online hoax about a chemical explosion at Columbian Chemical Plant in Centerville, Louisiana on the anniversary of the attacks of September 11, 2001. According to an investigation by the New York Times Magazine, the campaign was highly coordinated and included dozens of fake Twitter accounts that posed as local eyewitnesses and residents, faux websites masquerading as local Louisiana news outlets, and other fabricated evidence. The IRA-linked accounts posted hundreds of tweets with the hashtag #ColumbianChemicals to amplify the nonexistent explosion—many of which included falsified eyewitness testimonies, videos, and news articles—as well as contacted local journalists, media outlets, and politicians to alert them about the "news". Some of the fake IRA accounts even tried to connect the disaster to the Islamic State group (IS), amplifying a YouTube video also fabricated by the IRA that purported to show IS claiming credit for the attack.

Chinese influence campaign claims COVID-19 originated from Maine lobsters

State: Maine

Threat Actor: China

Date: 2021

Objective: Distract

Select Channels & Affordances: Social Media Platforms, Traditional Media, and Formal Diplomatic Channels

Tactics & Techniques: Develop Narratives (develop original conspiracy theory narratives); Develop Content (distort facts and reframe context), Establish Assets (compromised assets and pre-existing assets), Establish Legitimacy (fabricated and impersonated personas), Conduct Pump Priming (seed distortions), Maximize Exposure (post across platform and trolls amplify and manipulate)

A pro-China influence campaign amplified a false claim suggesting that the COVID-19 pandemic originated from Maine lobsters. In September 2021, a network of more than 550 Twitter accounts shared nearly identical messages that claimed a shipment carrying Maine lobsters from the United States brought the virus to a seafood market in Wuhan. The network shared the post in multiple languages—including English, Spanish, French, Polish, Korean and even Latin—at approximately the same time (morning China Standard Time). The network was a combination of "sock puppet" accounts that had few or no followers and accounts that appeared authentic but had been hijacked to spread false or misleading information. Chinese government officials on Twitter and state-controlled media repeated the false claim, and the latter group has repeatedly suggested that the virus may have originated from frozen food imports.

A screenshot of a Chinese government official's tweet amplifying the false claim that COVID-19 originated from Maine lobsters.

Suspected foreign actor targets Maryland Senator with deepfake during Zoom call

State: Maryland

Threat Actor: Unknown (likely Russia, China, or Iran)

Date: September 2024

Objective: Degrade Adversary, Discredit, and Undermine (smear)

Select Channels & Affordances: Chat Platform and Email Platform

Tactics & Techniques: Develop Content (develop AI-generated audio and video); Establish Assets (AI-generated account imagery and email domain asset); Establish Legitimacy (impersonated persona)

In September 2024, an unknown malign actor used sophisticated deepfake technology to pose as a top Ukrainian official in a Zoom video call with Maryland Senator and chair of the Senate Foreign Relations Committee Ben Cardin. According to a notice on the incident, Cardin's office received an email that appeared to be from former Ukrainian Foreign Minister Dmytro Kuleba requesting to connect over Zoom. On the conference call, the impersonator—who used AI technology to both look and sound like Kuleba—raised suspicions after asking pointed questions about the 2024 presidential election and US policy on Ukraine, including whether the senator supported the use of long-range missiles in Russian territory. Senator Cardin promptly ended the call and reported the incident. Intelligence sources suspect involvement from foreign actors, most likely Russia, China, or Iran.

Network of AI-enhanced Russian websites pose as American newspapers, including Boston outlet

State: Massachusetts

Threat Actor: Russia

Date: 2024

Objective: Degrade Adversary and Undermine (smear and polarize)

Select Channels & Affordances: Website Assets and Social Media Platforms

Tactics & Techniques: Develop Narratives (develop original conspiracy theory narratives and leverage existing narratives); Develop Content (develop inauthentic news articles, documents, AI-generated text, and deceptively edit images and video); Establish Assets (develop owned media assets); Establish Legitimacy (create inauthentic news sites); Microtarget (create clickbait content); Conduct Pump Priming (seed distortions); Deliver Content (direct posting); Maximize Exposure (inauthentic sites amplify news and narratives)

A Russian state-sponsored operative employed AI to fabricate a network of at least 167 websites that masqueraded as local newspapers in the United States—including a faux Massachusetts outlet called the "Boston Times"—to influence public discourse about Ukraine and sway American voters ahead of the 2024 presidential election. The faux websites published stories that promoted Kremlin narratives, often with the intent to deceive and polarize American audiences. Examples of fabricated stories published on the network included a false allegation that the FBI wiretapped then-presidential candidate Trump and a fictitious accusation that Ukrainian First Lady Olena Zelenska used US military aid to purchase an Italian sports car. The false news stories often incorporated forged documents or fabricated videos to bolster the claims and/or were attributed to journalists who did not exist, using fictitious names and profile pictures taken from real people found online. The operation likely used AI to write fabricated stories or rewrite legitimate news stories with fake elements or a political stance. The operation published thousands of stories weekly, which were often republished across the websites in the network and amplified by bot accounts.

Covert Iran-controlled Detroit news site used to polarize Americans ahead of 2024 election

State: Michigan

Threat Actor: Iran

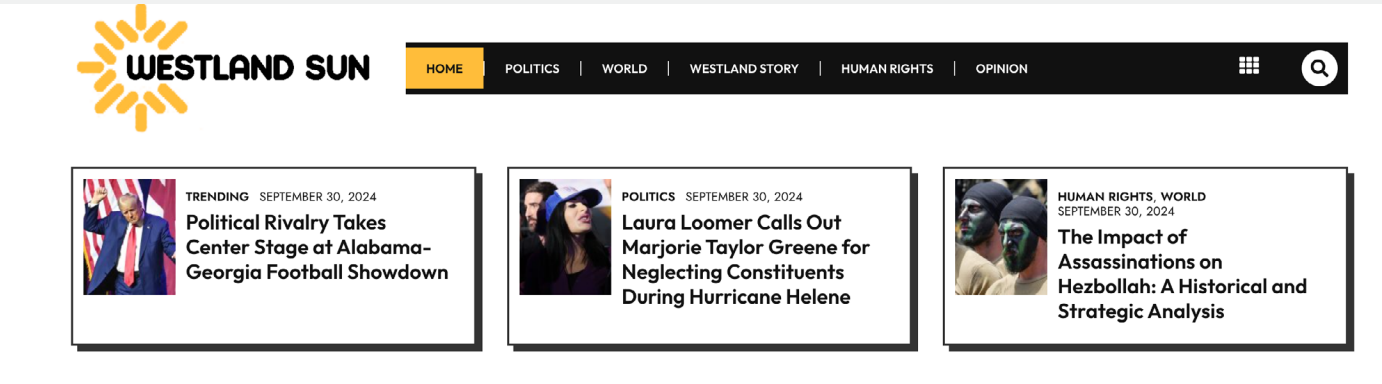
Date: 2023 – August 2024

Objective: Degrade Adversary and Undermine (smear and polarize)

Select Channels & Affordances: Website Assets

Tactics & Techniques: Develop Narratives (leverage existing narratives); Develop Content (create inauthentic news articles and AI-generated text); Establish Assets (establish newly created assets); Establish Legitimacy (create inauthentic news sites); Microtarget (create clickbait and localized content); Deliver Content (direct posting); Maximize Exposure (inauthentic sites amplify news and narratives); Persist in the Information Environment (conceal sponsorship)

An Iranian state-linked influence group operated a network of at least 19 fake websites posing as local news and media sites—including a Detroit news site called "Westland Sun"—to target specific voting demographics ahead of the 2024 US presidential election. Westland Sun appeared to cater to left-leaning audiences and Arab Americans in suburban Detroit, promoting content critical of US support for Israel and US democracy. For example, the website published an article entitled "The Democratic Party's Unwavering Commitment to Military Power: A Threat to Peace and Democracy". Other websites in the network targeted Americans on the other side of the political spectrum, including "Savannah Time", a fake Georgia website that described itself as "the trusted source for conservative news in the vibrant city of Savannah" and echoed right-wing criticism related to policies towards LGBTQ+ individuals and other gender issues. Many of the websites used artificial intelligence to generate content for the pages. OpenAI banned a set of accounts linked to the Iranian influence campaign that used ChatGPT to generate content for the websites in August 2024.



A screenshot of Westland Sun's homepage, which showcases stories promoting pro-Iranian narratives.

Foreign actors seize on George Floyd protests to sow division

State: Minnesota

Threat Actor: China, Iran, and Russia

Date: 2020

Objective: Divide, Undermine (polarize), and Distract

Select Channels & Affordances: Social Media Platforms, Traditional Media, and Formal Diplomatic Channels

Tactics & Techniques: Develop Narratives (leverage existing narratives and respond to breaking news event); Develop Content (develop memes and use existing hashtags); Establish Assets (pre-existing assets); Conduct Pump Priming (seed kernel of truth); Deliver Content (direct posting and share memes); Maximize Exposure (amplify existing narratives)

State-controlled media outlets and diplomatic accounts linked to China, Russia, and Iran seized on the killing of George Floyd and the subsequent Black Lives Matter (BLM) protests to stoke division and discredit the United States. Officials and state media in all three countries amplified coverage about Floyd's death and the BLM protests—in many cases wielding the movement's hashtags, mottos, and imagery—to portray the United States as hypocritical and in turmoil. Chinese officials and state-controlled media frequently drew comparisons between the US government's response to the BLM demonstrations and the crackdown on pro-democracy protests in Hong Kong. In one of the most-shared tweets by a Chinese official following Floyd's death, spokeswoman for China's Foreign Ministry of Affairs Hua Chunying exploited Floyd's last words, "I can't breathe", to mock a US State Department official's criticism of China's treatment of Hong Kong. Iranian state actors similarly capitalized on the protests to undermine Trump—amplifying a cartoon image of Trump kneeling on Floyd alongside the caption "George Floyd, a new crime of Trump's regime"—to call out the United States' alleged double standards on human rights.

Tweet of Chinese Ministry of Foreign Affairs spokesperson using BLM mottos to stoke division and discredit the United States.

Russian cyberattack takes down Mississippi government websites on Election Day

State: Mississippi

Threat Actor: Russia

Date: November 9, 2022

Objective: Degrade Adversary, Cause Harm (intimidate), and Undermine (subvert)

Select Channels & Affordances: Social Media Platforms

Tactics & Techniques: Develop Content (develop memes); Establish Assets (pre-existing assets); Conduct Pump Priming (seed distortions); Deliver content (direct posting); Drive Online Harms (control information environment through offensive cyberspace operations)

The pro-Russian hacking group Cyber Army of Russia Reborn took down multiple websites operated by the Mississippi Secretary of State's office for several hours on the day of the 2022 midterm election. The attack did not compromise voting technology but prevented voters from accessing web pages that included voting and polling place information. Months earlier, a different pro-Russian group, Killnet, claimed responsibility for a cyberattack that also took several state government websites, including those in Mississippi, Colorado, and Kentucky, offline for several hours. Killnet had previously listed US state websites among its targets for cyberattacks on Telegram, beneath a picture reading "F-NATO."

Russian agents funded and directed black activists in St. Louis to sow discord and spread Kremlin propaganda

State: Missouri

Threat Actor: Russia

Date: 2015 – 2022

Objective: Cultivate Support (recruit members), Motivate to Act (encourage), and Divide

Select Channels & Affordances: Direct Messaging and Formal Diplomatic Channels

Tactics & Techniques: Target Audience Analysis (identify existing fissures); Develop Narratives (leverage existing narratives); Develop Content (develop document); Establish Assets (recruit partisans); Establish Legitimacy (co-opt grassroots groups); Deliver Content (attract traditional media); Drive Offline Activity (encourage attendance at events); Persist in the Information Environment (obfuscate payments)

In September 2024, four members of the African People's Socialist Party (APSP)—a Black activist group operating in St. Louis, Missouri and St. Petersburg, Florida—were convicted of conspiracy to act as unregistered Russian agents to help the Kremlin sow political discord and spread propaganda between 2015 and 2022. (They were acquitted of the more serious charge of working as foreign agents.) Three of the four APSP members, including founder Omali Yeshitela, resided in St. Louis. According to the charges, the APSP members knowingly received funds and instructions from Aleksandr Ionov, a Russian national accused of working under the direction of Russian intelligence, to stage protests and perform actions that aligned with the Kremlin's interests. Notably, this included drafting and submitting a petition to the United Nations in 2015 that charged the United States with actively committing genocide against African people. Ionov subsequently provided the members $12,000 to fund a four-city tour to promote the genocide petition. In 2020, Ionov invited Yeshitela and APSP member Jesse Nevel to speak at a conference to promote the right of self-determination for Russian-backed secessionist movements in Eastern Ukraine.

Chinese state media denigrates Montana and United States for TikTok ban

State: Montana

Threat Actor: China

Date: April - May 2023

Objective: Dissuade from Acting (discourage), Divide, and Undermine (thwart)

Select Channels & Affordances: Social Media Platforms, Traditional Media, Formal Diplomatic Channels

Tactics & Techniques: Develop Narratives (leverage existing narratives and develop new narratives); Develop Content (develop opinion articles); Deliver Content (direct posting); Maximize Exposure (amplify existing narrative)

After Montana's legislature approved a law to ban TikTok from operating in the state, PRC state media capitalized on the decision to push denigrating narratives about Montana and the United States. Chinese state media called out Washington's "double standards" in protecting freedom of speech and claimed Montana was attempting to "censor American voices". The Global Times suggested that Montana's ban was rooted in anti-Asian racism and professed that the United States was entering an "age of barbarism". China Daily similarly published an article alleging that the ban is evidence of "systemic fraud" caused by US hegemony. PRC messaging further tried to paint American discontent about the bill, claiming it triggered an "outcry" and amplifying comments by a Montana citizen that the ban is a threat to their "livelihood".

A Global Times cartoon denigrating the United States over Montana's TikTok ban.

Chinese hackers hijack Twitter account of Nebraska student to disseminate propaganda

State: Nebraska

Threat Actor: China

Date: January – March 2020

Objective: Cultivate Support (defend reputation) and Facilitate State Propaganda

Select Channels & Affordances: Social Media Platforms

Tactics & Techniques: Develop Narratives (leverage existing narratives); Develop Content (create inauthentic news articles and AI-generated text); Establish Assets (compromised assets); Establish Legitimacy (authentic persona); Deliver Content (direct posting and inauthentic social media comments); Maximize Exposure (trolls amplify and manipulate); Persist in the Information Environment (change names of information assets)

In January 2020, Chinese state-linked hackers hijacked the Twitter account of a University of Nebraska Omaha student and turned it into a "zombie account" to spread propaganda. According to an investigation by ProPublica, the hacked account aggressively published tweets in both Chinese and English on topics that aligned with Chinese Communist Party interests, including the 2019 protests in Hong Kong—frequently praising Hong Kong police—and the COVID-19 pandemic. A month after the hack, the hijacked profile started to distance itself from the original user, changing the account's name, picture, and biography. More than 10,000 suspected fake Twitter profiles with ties to the Chinese government have been identified by ProPublica since August 2019. Among those are hacked accounts of users from around the world, including a professor in North Carolina; a graphic artist and a mother in Massachusetts; a web designer in the United Kingdom; and a business analyst in Australia.

Russian-affiliated media circulate false theories about Las Vegas shooting

State: Nevada

Threat Actor: Russia

Date: October 2017

Objective: Divide and Undermine (polarize)

Select Channels & Affordances: Website Assets, Traditional Media, and Social Media Platforms

Tactics & Techniques: Develop Narratives (leverage conspiracy narratives and respond to breaking news event); Develop Content (text-based); Establish Assets (pre-existing assets and fund proxies); Conduct Pump Priming (seed distortions); Deliver Content (direct posting); Maximize Exposure (amplify existing narratives)

In the aftermath of a mass shooting in Las Vegas in 2017, outlets affiliated with Russia created and circulated false theories about the tragedy. Veterans Today—a fringe American outlet that caters to retired veterans and has ties to Russian organizations—published an article suggesting that the Las Vegas shooting was a "false flag" operation to expand government power and strip Americans' rights. The Strategic Culture Foundation, a Russian think tank sanctioned for spreading false information, similarly published a speculative article that sought to cast doubt about the tragedy's facts, including insinuating US government involvement in the Vegas shooting, as well as other mass shootings like Sandy Hook. Russian state media outlet Sputnik also published an article with the headline "FBI Says Las Vegas Shooter Has Connection with Daesh Terror Group", which Forbes flagged. Sputnik claimed that the headline was "published with a typo" and was originally missing the word "no" and accused Forbes of blowing the mistake out of proportion.

Chinese state-sponsored Confucius Institutes maintain presence at US college campuses, including University of New Hampshire

State: New Hampshire

Threat Actor: China

Date: 2004 - Present

Objective: Cultivate Support (boost reputation) and Dissuade from Acting (silence)

Select Channels & Affordances: Offline

Tactics & Techniques: Establish Assets (create organization)

Since 2004, the Chinese government has sponsored Confucius Institutes—a public education and Chinese cultural program—on college and university campuses around the world, including the University of New Hampshire, that were used to promote propaganda and encourage censorship on sensitive Chinese issues overseas. While the majority of Confucius Institutes in the United States since have closed—104 of 118 have shut down—many have reopened or rebranded under new names. According to an investigation by the National Association of Scholars (NAS), at least 28 universities and colleges have replaced their Confucius Institute with a similar partnership (including signing new agreements with the Center for Language Exchange and Cooperation, the successor to Hanban, the Confucius Institute's parent organization), and 58 have maintained close relationships with their former Confucius Institute partner. The University of New Hampshire opened its Confucius Institute in 2010 and ended its program in 2021, citing "a series of probes/inquiries/investigations from the Justice, Education as well as the State Department". Since closing, NAS has noted that the University of New Hampshire has maintained an exchange program and "cooperative PhD" partnership with its Confucius Institute partner.

China hires New Jersey media company to recruit American influencers

State: New Jersey

Threat Actor: China

Date: January - March 2022

Objective: Cultivate Support (cultivate support for an initiative)

Select Channels & Affordances: Social Media Platforms

Tactics & Techniques: Develop Narratives (develop new narratives); Develop Content (video-based); Establish Assets (cultivate ignorant agents and outsource content creation to external organization); Establish Legitimacy (co-opt influencers); Deliver Content (direct posting); Persist in the Information Environment (conceal sponsorship)

The Chinese Consulate in New York paid the New Jersey-based firm Vippi Media $300,000 to recruit social media influencers to promote the 2022 Beijing Winter Olympics. According to filings disclosed with the Justice Department, Vippi Media enlisted 11 brands and influencers—including a "Real Housewives of Beverly Hills" star and an American paralympic athlete—to create crafted videos promoting the Olympics tailored to their specific audiences. The influencer posts were marketed as advertisements and often included the hashtags #Beijing2022, #partner, and #ad. The social media posts appeared across a variety of platforms, including Instagram, YouTube, and TikTok and generated 3.8 million impressions. In one post, a content creator with more than half a million followers posted a three-minute-long interview with China's Consul General in New York in which the two criticized US tariffs against Chinese imports. Although the payments to influencers were disclosed under the Foreign Agents Registration Act, the social media users themselves were frequently unaware of the source of funds for their sponsored content.

Chinese "Wolf Warrior" amplifies Albuquerque resident's tweet to promote claims about COVID-19 State

State: New Mexico

Threat Actor: China

Date: March 2020

Objective: Distract

Select Channels & Affordances: Social Media Platform and Formal Diplomatic Channels

Tactics & Techniques: Develop Narratives (leverage existing narratives); Establish Legitimacy (co-opt trusted individuals); Maximize Exposure (amplify existing narrative)

In March 2020, a prominent Chinese government official amplified a tweet by a New Mexico resident to sow doubt about COVID-19's origins. The original tweet—written by a young mother in Albuquerque with only a few hundred followers—speculated that COVID-19 materialized in the United States earlier than officials let on. A week later, Zhao Lijian, the spokesperson for China's Foreign Ministry of Affairs at the time, retweeted her post. The post received more than 7,000 likes and over 2,300 retweets. Zhao Lijian was one of China's most prominent "Wolf Warriors" on Twitter", employing his account to aggressively promote and post pro-China propaganda. During the COVID-19 pandemic, Zhao Lijian and other "Wolf Warriors" made a concerted effort to push false claims about the virus' origin, including that it was engineered as a bioweapon by the United States at Fort Detrick army research facility.

Former aide to two New York governors charged with being Chinese agent

State: New York

Threat Actor: China

Date: 2012 - 2023

Objective: Cultivate Support and Dissuade from Acting (discourage)

Select Channels & Affordances: Offline

Tactics & Techniques: Establish Assets (recruit malign actors); Establish Legitimacy (co-opt trusted individuals)

In September 2024, a federal court in Brooklyn unveiled charges against Linda Sun, a former aide to New York Governor Kathy Hochul and former Governor Andrew Cuomo, for acting as an illegal foreign agent of China. According to the indictment, Sun used Chinese money and her influence within the state of New York to covertly advance Chinese state interests in exchange for financial benefits worth millions of dollars. The charges allege that Sun engaged in numerous political activities, including shaping government messaging on issues of importance to China, blocking representatives from Taiwan from having access to state officials, and facilitating meetings between New York politicians and Chinese delegations. In several cases, Sun eliminated references to Taiwan and the Uyghurs from state communications.

Russia, China, and Cuba spread false and polarizing information about hurricane relief

State: North Carolina

Threat Actor: Russia; China; Cuba

Date: September - October 2024

Objective: Divide and Undermine (smear and polarize)

Select Channels & Affordances: Website Assets, Social Media Platforms, Traditional Media

Tactics & Techniques: Develop Narratives (leverage existing narratives and amplify existing conspiracy narratives); Develop Content (develop AI-generated images); Establish Assets (pre-existing assets); Microtarget (create clickbait and localized content); Deliver Content (direct posting); Maximize Exposure (bots amplify via automated forwarding and reposting)

Russian, Chinese, and Cuban operatives all spread false, misleading, and polarizing narratives about Hurricanes Helene and Milton and the US government's relief efforts. The three countries used state media and bot networks to amplify narratives that had gained traction online with American users, including false accusations that federal disaster funds were diverted to support foreign conflicts and migrants. In one case, the Russian state-owned news agency RIA Novosti shared an AI-generated image on Telegram that purported to show a flooded Disney World. Chinese state-linked actors similarly circulated an image likely generated by AI that portrayed Harris overlooking flood damage next to a sign, which stated that all the United States' money went to Ukraine, Israel, and Taiwan. The Federal Emergency Management Agency has warned that false information about the disaster by both domestic and foreign actors could hamper recovery efforts.

An RT tweet amplifying false claims about hurricane recovery.

Russia's IRA uses fake social media accounts and pages to amplify discontent about Dakota Access Pipeline

State: North Dakota

Threat Actor: Russia

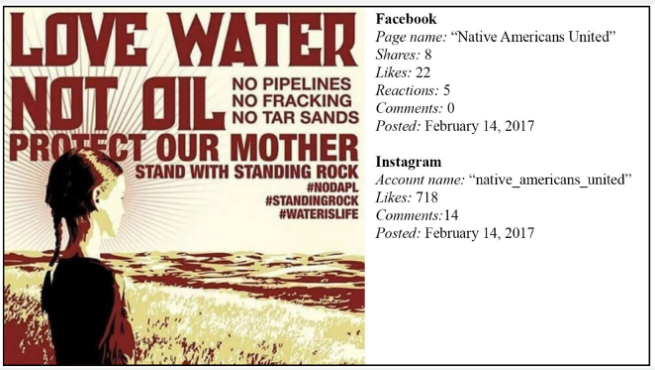
Date: 2015—2017

Objective: Divide, Dissuade from Acting (Deter), and Undermine (polarize and thwart)

Select Channels & Affordances: Social Media Platforms

Tactics & Techniques: Develop Narratives (leverage existing narratives); Develop Content (develop memes and text-based content); Establish Assets (newly created assets and create community or sub-groups); Establish Legitimacy (fabricated and social cause personas); Deliver Content (direct posting, share memes, and comment or reply on content); Maximize Exposure (trolls amplify and manipulate)

Russia's Internet Research Agency (IRA) sought to further polarize Americans on sensitive environmental issues, including the Dakota Access Pipeline (DAPL). According to a 2018 report by the House Committee on Science, Space, and Technology, an estimated 4,334 Twitter, Facebook, and Instagram accounts linked to the IRA shared over 9,000 posts regarding US energy policy or environmental issues. The report notes that the IRA in particular exploited controversy over the DAPL, amplifying narratives both for and against its construction. Notably, the IRA-run account "Native Americans United" amplified discontent among indigenous communities about the pipeline, posting images of young Native American girls with captions such as "I need water not oil" or "Only in America are water protectors treated as terrorists". Other pages amplified content about DAPL protests, including encouraging the protests or emphasizing and exacerbating their alleged violent nature.



Posts by IRA-controlled accounts targeting audiences on both sides of the DAPL controversy.

(Source: House Committee on Science, Space, and Technology report)

Pro-Russian X accounts stoke fear and distrust about Ohio train disaster

State: Ohio

Threat Actor: Russia

Date: February 2023

Objective: Divide and Undermine (polarize)

Select Channels & Affordances: Social Media Platforms

Tactics & Techniques: Develop Narratives (leverage existing narratives, develop original conspiracy theory narratives, respond to breaking news event); Develop Content (text and image-based and create fake research); Establish Assets (verified account assets and pre-existing assets); Conduct Pump Priming (seed distortions); Deliver Content (direct posting)

In February 2023, a network of anonymous pro-Russian X accounts capitalized on the train derailment in East Palestine, Ohio to stoke fear and mistrust in state and federal authorities. The accounts falsely claimed that authorities in Ohio were covering up the true impact of the spill and spread fear-mongering posts that preyed on legitimate concerns about pollution and health effects from the disaster, including posting images of unverified maps allegedly depicting the scope of pollution, speculating increases in cancer diagnoses, and reporting unconfirmed mass animal die-offs. Some accounts even pushed false theories, including suggesting that environmental scientists traveling to the disaster site had been killed in a plane crash. Other accounts tried to juxtapose the United States' response to the disaster with President Joe Biden's support for Ukraine. For example, one account with 25,000 followers tweeted "Biden offers food, water, medicine, shelter, payouts of pension and social services to Ukraine! Ohio first! Offer and deliver to Ohio!" Most of the Russian-linked accounts carried a blue check mark, exploiting X's new pay-for-account-verification policy to appear more authoritative.

Chinese influence campaign targets Western mining and rare earth firms, including one seeking to expand to Oklahoma

State: Oklahoma

Threat Actor: China

Date: 2022

Objective: Cause Harm (defame) and Undermine (smear)

Select Channels & Affordances: Social Media Platforms

Tactics & Techniques: Develop Narratives (develop new narratives); Develop Content (text-based); Establish Assets (pre-existing assets); Establish Legitimacy (fabricated and local personas); Microtarget (create localized content); Conduct Pump Priming (seed kernel of truth); Deliver Content (direct posting); Maximize Exposure (trolls amplify and manipulate and bots amplify via automated forwarding and reposting); Drive Offline Activity (call to action to attend event)

In 2022, a Chinese state-linked network launched an online influence campaign intended to undermine Western firms that mine and process rare-earth elements, including two different companies after they announced that they were opening facilities in Texas and Oklahoma, respectively. According to the cybersecurity firm Mandiant, which discovered the campaign, the network first targeted the Australian company Lynas Rare Earths Ltd, by employing inauthentic social media and forum accounts to criticize the company's alleged environmental record and encourage protests against the planned construction of its new rare earths processing facility in Texas. Some of the bot accounts posed as local Texas residents. In early June, the campaign similarly targeted the American company USA Rare Earth after it announced plans to open a processing facility in Oklahoma. The activity reportedly did not appear to have been particularly effective and received limited engagement by seemingly real individuals.

Russian state-linked actors exploit 2020 Portland unrest to stoke division

State: Oregon

Threat Actor: Russia

Date: August 2020

Objective: Divide and Undermine (polarize)

Select Channels & Affordances: Traditional Media, Video Platforms, Social Media Platforms

Tactics & Techniques: Develop Narratives (leverage existing narratives and respond to breaking news event); Develop Content (deceptively edit videos); Microtarget (create clickbait and localized content); Conduct Pump Priming (seed kernel of truth); Deliver Content (direct posting)

Russian state-linked actors amplified genuine and manipulated coverage of unrest during the 2020 Portland protests to sow political division. According to an investigation by the New York Times, Ruptly, a video news subsidiary of the Russian state-controlled media outlet RT, edited and promoted a misleading video of Portland protesters burning a Bible that falsely exaggerated the scale of the incident, including misconstruing the video to make it appear as if the burning was the event's main attraction and that more people participated, and removing footage of other protesters attempting to put out the fire. An American videographer admitted he was paid up to $400 for footage of the protests and that Ruptly requested he specifically provide coverage of authorities "beating the crap out of protesters" and "protesters lighting stuff on fire, riots". Social media accounts with ties to Russia's Ministry of Foreign Affairs also tried to promote violence against demonstrators, including posting a cartoon image of a driver running over a protester with the caption "don't break for communists" and content calling for a "civil war" against Antifa and the Black Lives Matter movement.

Russian state-linked influence operation disseminates video falsely depicting ballots being destroyed in Bucks County, PA

State: Pennsylvania

Threat Actor: Russia

Date: October 2024

Objective: Divide and Undermine (polarize)

Select Channels & Affordances: Video Platforms and Social Media Platforms

Tactics & Techniques: Develop Narratives (develop original conspiracy theory narratives); Develop Content (deceptively edit video); Establish Assets (pre-existing assets); Microtarget (create clickbait); Deliver Content (direct posting); Maximize Exposure (trolls amplify and manipulate)

Two weeks before the 2024 presidential election, the Russian state-linked influence network Storm-1516 manufactured and amplified a video that purported to show mail-in ballots marked for Trump being destroyed in Bucks County, Pennsylvania. The fake video depicted a person, who was Black, sorting through mail-in ballots labeled as coming from Bucks County and tearing up ballots marked for Trump, while leaving ballots marked for Harris alone. Bucks County election officials debunked the video within three hours, but it was still widely circulated on social media, notably on X, where it amassed hundreds of thousands of views. ODNI, FBI, and CISA released a joint statement, which explained that the video was part of Russia's larger campaign to undermine confidence in US elections and deepen divisions among Americans.

Iran and other foreign state-linked actors amplify unrest on college campuses over Israel-Gaza conflict

State: Rhode Island

Threat Actor: Iran; Russia; China

Date: 2024

Objective: Degrade Adversary, Divide, and Undermine (polarize)

Select Channels & Affordances: Traditional Media and Social Media Platforms

Tactics & Techniques: Develop Narratives (leverage existing narratives); Develop Content (text-based and video-based); Establish Legitimacy (co-opt grassroots movements); Maximize Exposure (amplify existing narrative)

Foreign state-linked actors in Iran, Russia, and China have amplified college campus protests about the Israel-Gaza conflict, including student discontent at Brown University in Rhode Island, to stoke division and discredit the United States. Iranian state-controlled outlets took a notable interest in student actions at Brown University. PressTV, Iran's English-language international outlet, promoted videos of campus demonstrations—including a student coalition hunger strike—calling for Brown University to divest from companies profiting from the conflict. Many of the posts used the hashtags #WeAreAllGaza or #GazaGenocide. Following an agreement between student protesters and the university to halt divestments, Iranian state media painted the decision as a "victory" for the student protesters and said Brown "succumbed" to the "resistance of American students".

Russian state-backed troll farm in Ghana amplifies racial division, tries to recruit Charleston activists

State: South Carolina

Threat Actor: Russia

Date: 2019 - 2020

Objective: Divide and Undermine (polarize)

Select Channels & Affordances: Social Media Platforms and Encrypted Communication Channels

Tactics & Techniques: Develop Narratives (leverage existing narratives); Develop Content (text-based content and develop memes); Establish Assets (create content farms, cultivate ignorant agents, and bulk created assets); Establish Legitimacy (fabricated and activist personas); Deliver Content (direct posting); Maximize Exposure (trolls amplify and manipulate and posting across platforms); Persist in the Information Environment (conceal sponsorship and coordinate on encrypted/closed networks)

A Russian state-backed troll farm based in Ghana amplified divisive narratives about racial issues and tried to hire on-the-ground activists in South Carolina, according to a CNN investigation. The troll farm, which operated under the guise of a small non-profit called "Eliminating Barriers for the Liberation of Africa" (EBLA) in Ghana's capital Accra, focused almost exclusively on racial issues in the United States, promoting Black empowerment and often displaying anger towards white Americans. All of EBLA's funding reportedly came from Russia and links were found between the campaign and the Internet Research Agency. EBLA employees—who were both witting and unwitting Ghanaian nationals—were guided on encrypted Telegram channels about what topics to post about. Facebook told CNN that 13,200 Facebook accounts followed one or more of the Ghanaian troll farm accounts and around 263,200 people followed one or more of its Instagram accounts, about 65% of whom were in the United States. Twitter removed 71 accounts linked to the Ghanaian troll farm that had 68,000 total followers. In late January of 2020, EBLA advertised for a "chapter coordinator" position in Charleston, South Carolina. The LinkedIn posting invited applicants to "join hands with our brothers and sisters world-wide, especially in the United States where POC [people of color] are mostly subjected to all forms of Brutality."

Convicted Russian agent forged relationships with Americans and universities in South Dakota

State: South Dakota

Threat Actor: Russia

Date: 2014 - 2015

Objective: Cultivate Support

Select Channels & Affordances: Offline

Tactics & Techniques: Establish Assets (cultivate ignorant agents); Establish Legitimacy (co-opt trusted individuals)

Maria Butina—a convicted Russian agent—began her years-long campaign to infiltrate US conservative organizations in South Dakota. According to investigations, Butina spent her time living in Sioux Falls in 2014 and 2015, where she cultivated relationships with conservative Americans across the state, including speaking at a South Dakota Teen Republicans summer camp and a finance workshop for high schoolers in Sioux Falls and giving a guest lecture on gun rights at the University of South Dakota. A flyer for her event at the University of South Dakota portrayed her as the face of Russia's gun-rights movement. All three events were organized with the help of Paul Erickson, a South Dakota Republican and political operative whom Butina was dating at the time. Erickson assisted Butina's campaign by introducing her to powerful political figures and groups. Butina's time connecting at the local level in South Dakota is believed to have been used to gather information on sensitive US issues and to establish her professional track record.

Chinese influence network seeks to undermine Tennessee candidate ahead of 2024 elections

State: Tennessee

Threat Actor: China

Date: 2024

Objectives: Undermine (smear opponents)

Select Channels & Affordances: Social Media Platforms

Tactics & Techniques: Develop Narratives (leverage existing narratives); Develop Content (text-based); Establish Assets (pre-existing assets); Deliver Content (direct posting); Microtarget (create localized content); Maximize Exposure (utilize Spamouflage)

A Chinese state-linked influence operation attempted to denigrate Republican Senator Marsha Blackburn of Tennessee and congressional candidates in other states to sway down-ballot races. In the months leading up to the 2024 elections, the influence network Spamouflage employed dozens of inauthentic accounts to post negative content about congressional candidates who were critics of the Chinese government. According to Microsoft, which identified the operation, the bot accounts attempted to undermine Blackburn's candidacy by spreading claims of corruption, including that Blackburn took money from pharmaceutical companies, and promoting her opponent. The campaign tried to amplify its content by tagging prominent politicians, celebrities, and news outlets in relevant posts, but none of the posts received a high level of engagement. Other targeted members of Congress in the operation included Alabama Representative Barry Moore, Florida Senator Marco Rubio, and Texas Representative Michael McCaul—all Republicans.

Russian influence campaign amplifies calls for "Civil War" over Texas border crisis

State: Texas

Threat Actor: Russia

Date: January 2024

Objectives: Divide and Undermine (polarize)

Select Channels & Affordances: Social Media Platforms, Traditional Media, and Formal Diplomatic Channels

Tactics & Techniques: Develop Narratives (leverage existing narratives and develop new narratives); Develop Content (develop AI-generated content); Establish Assets (pre-existing assets); Conduct Pump Priming (seed distortions); Deliver Content (direct posting); Maximize Exposure (bots amplify via automated reposting and forwarding)

In January 2024, Russian state-backed operatives seized on the feud between Texas and federal authorities over how to tackle the migrant crisis on the US-Mexico border to coordinate an influence campaign aimed at sowing discord over the crisis, including boosting narratives suggesting the United States is headed towards civil war. Deputy Chairman of the Security Council of the Russian Federation Dmitry Medvedev (also a former Russian president and prime minister) and other government officials claimed that the Texas border crisis underscores Washington's decline, and suggested it could result in a "bloody civil war" and Texas' secession. These narratives were subsequently amplified by Russian bot-networks, influencers, and state media. For example, RT and other Russian media outlets published a flood of articles with headlines featuring phrases like "Civil War 2.0"; Russian TV personality Vladimir Solovyov, who has more than 1.2 million followers on Telegram, claimed, "The US was close to civil war". A video of Texas Governor Greg Abbott was also digitally altered using AI so that some of his comments on border policy were replaced with Abbott saying Biden could learn from Russian President Vladimir Putin. That post received over 130,000 views.

A screenshot of an AI-altered video of Texas Governor Greg Abbott.

China conducts years-long campaign to influence Utah officials

State: Utah

Threat Actor: China

Date: 2007 - Present

Objectives: Cultivate Support (boost reputation)

Select Channels & Affordances: Offline

Tactics & Techniques: Establish Legitimacy (co-opt trusted sources)

Since 2007, Chinese government officials and organizations have administered a widespread influence campaign targeting Utah lawmakers to guide state policy and messaging on China. According to an Associated Press investigation, the campaign tried to cultivate relationships with Utah lawmakers by sponsoring their travel to China, facilitating meetings between them and Chinese government officials, arranging for their coverage in state-controlled media, and even trying to appeal to their affiliations with the Church of Jesus Christ of Latter-day Saints. The campaign has reportedly resulted in lawmakers delaying or blocking legislation critical of China, including a ban on Confucius Institutes and a resolution condemning the crackdown on China's Uyghur population. The campaign is a part of a larger effort by China to redouble its influence at the local level in the face of growing resistance in Washington.

Russian influence campaign tries to boost Vermont Senator in presidential race

State: Vermont

Threat Actor: Russia

Date: 2016 and 2020

Objectives: Divide and Undermine (smear)

Select Channels & Affordances: Social Media Platforms and Traditional Media

Tactics & Techniques: Develop Narratives (leverage existing narratives); Develop Content (develop memes and text-based content); Establish Assets (create community or sub-group and newly created assets); Establish Legitimacy (fabricated, activist, and social cause personas); Deliver Content (direct posting and deliver social media ads); Microtarget (purchase targeted advertisements); Maximize Exposure (trolls amplify and manipulate and bots amplify via automated forwarding and reposting)

Russian state-sponsored actors promoted Vermont Senator Bernie Sanders during the 2016 and 2020 Democratic presidential primaries. As a part of its effort to divide Americans ahead of the 2016 presidential election, fake social media accounts and paid advertisements linked to Russia's Internet Research Agency (IRA) amplified support for Sanders while denigrating his opponent, Hillary Clinton. The campaign to promote Sanders often targeted specific voter demographics, including the LGBTQ+ and Muslim communities. For example, a Russian-run account called "LGBT United" purchased a Facebook advertisement for a coloring book called "Buff Bernie" that depicted an image of Sanders wearing a speedo and with generous muscles. Another IRA account called "Missouri News" posted pictures of Sanders and President Franklin Roosevelt with the line "Bernie Sanders is basically a New Deal Democrat, #feeltheBern". In 2020, US officials briefed Sanders that Russian state actors were similarly trying to boost his campaign. Russian state media messaging on Sanders was overwhelmingly positive that year, too. Sanders received two and a half times more positive coverage than any other Democratic candidate, and even more than Trump, according to data from the Foreign Policy Research Institute. Sanders publicly condemned Russia for exploiting his campaign to interfere in the 2020 election.

Facebook advertisement bought by an IRA account boosting Bernie Sanders' 2016 campaign.

Pro-Russian bots amplify right-wing extremism about Charlottesville rally

State: Virginia

Threat Actor: Russia

Date: August 2017

Objectives: Cause Harm (spread hate), Divide, and Undermine (polarize)

Select Channels & Affordances: Social Media Platform

Tactics & Techniques: Develop Narratives (leverage existing and conspiracy theory narratives); Develop Content (develop memes and text-based content); Establish Assets (pre-existing assets); Establish Legitimacy (fabricated and social cause personas) Deliver Content (direct posting and comment or reply on content); Maximize Exposure (trolls amplify and manipulate and bots amplify via automated forwarding and reposting)

A Russian state-linked Twitter bot network amplified right-wing extremism and baseless theories following the violent "Unite the Right" rally in Charlottesville in August 2017. These accounts tried to blame the violence on liberal counterdemonstrations, including by promoting the hashtag "antifa" and falsely claiming George Soros organized them. One fake Twitter account posing as an American Christian conservative by the name of Angee Dixson posted nearly 90 times a day. The Angee Dixson spoof account—which has since been removed—defended Trump's response to the unrest in Charlottesville, criticized the removal of Confederate monuments, and posted pictures purporting to show violence by left-wing counter-protesters.

Examples of posts by Russian bot Angee Dixson account.

Indian state-linked influence operation smears Modi's critics in United States, including a Washington Representative

State: Washington

Threat Actor: India

Date: 2020 - Present

Objectives: Cause Harm (defame) and Undermine (smear)

Select Channels & Affordances: Social Media Platforms

Tactics & Techniques: Develop Narratives (develop new narratives); Develop Content (create fake research); Establish Assets (outsource content creation to external organization); Establish Legitimacy (co-opt influencers); Conduct Pump Priming (use fake experts); Deliver Content (direct posting); Microtarget (purchase targeted advertisements); Maximize Exposure (trolls amplify and manipulate and bots amplify via automated forwarding and reposting); Persist in the Information Environment (conceal sponsorship, distant reputable individuals from the operation, and deny involvement)

Since 2020, a research organization with links to Indian intelligence orchestrated a covert influence campaign targeting US-based critics of Indian Prime Minister Narendra Modi, including Democratic Representative Pramila Jayapal of Washington. The organization, Disinfo Lab, publishes and amplifies unsubstantiated research about US government officials, researchers, humanitarian groups, and Indian-American activists who are critical of Modi's government, often alleging that they are a part of a conspiracy—purportedly funded by Pakistani intelligence, the Muslim Brotherhood, and George Soros—to undermine India. These allegations regularly go viral on Indian social media after being amplified by prominent pro-Modi influencers. Although Disinfo Lab claims to be independent, it was reportedly set up and is run by an Indian intelligence officer, according to an investigation by the Washington Post. In June 2023, Disinfo Lab falsely targeted Jayapal, who is Indian-American. After Jayapal organized House and Senate members to write a letter urging Biden to address human rights issues with Modi before his visit to Washington, DC, Disinfo Lab published a thread on X that claimed she was influenced by Pakistan and Islamist funding. The post was retweeted more than 1,000 times.

Russia laundered $10M to unwitting American influencers, including West Virginia podcaster

State: West Virginia

Threat Actor: Russia

Date: 2024

Objectives: Divide, Undermine (polarize), and Degrade Adversary

Select Channels & Affordances: Social Media and Video Platforms

Tactics & Techniques: Develop Narratives (leverage existing narratives and develop new narratives); Develop Content (video-based content); Establish Assets (cultivate ignorant agents and develop owned media asset); Establish Legitimacy (co-opt influencers); Deliver Content (direct posting); Persist in the Information Environment (conceal sponsorship and obfuscate payment)

A Russian state-backed influence operation funded and directed an American media company that contracted unwitting content creators with large audiences, including an influencer based in West Virginia. In September 2024, the DOJ charged two Russian employees with conspiracy to violate the Foreign Agents Registration Act and conspiracy to commit money laundering in an elaborate scheme to influence Americans ahead of the 2024 presidential election. According to the indictment, RT employees Kostiantyn Kalashnikov and Elena Afanasyeva funneled nearly $10 million to an unnamed Tennessee company—later confirmed to be Tenet media—to publish English-language videos that echoed Russian talking points, including a conspiracy theory that the United States and Ukraine orchestrated the 2024 terrorist attacks in Moscow, and amplified "domestic division" in the United States. The owners of Tenet Media were allegedly both aware of and attempted to conceal the fact that they were being funded by Russian operatives. However, the indictment clearly states that the contributors to the platform—including West Virginia-based Tim Pool and other conservative content creators like Benny Johnson and Dave Rubin—were unaware of Tenet's Russian backing. All three influencers released statements saying they were victims and had no knowledge of the Kremlin scheme.

Russia creates and spreads fake video depicting voter being assaulted at Wisconsin polling station

State: Wisconsin

Threat Actor: Russia

Date: November 5, 2024

Objectives: Divide and Undermine (polarize)

Select Channels & Affordances: Social Media Platforms and Video Platforms

Tactics & Techniques: Develop Narratives (develop new narratives); Develop Content (deceptively edit video); Establish Assets (pre-existing assets); Establish Legitimacy (fabricated local personas); Deliver Content (direct posting); Maximize Exposure (trolls amplify and manipulate and bots amplify via automated forwarding and reposting)

The Russian-linked influence network known as Storm-1516 fabricated and disseminated a video purporting to show a voter being assaulted at a Wisconsin polling station on the day of the 2024 presidential election. The video, which has no sound, shows an individual in a hoodie marked "Harris" confronting an individual in a red pro-Trump "Make America Great Again" hat as he casts his vote. The supposed Trump supporter is then taken off camera and thrown to the floor by a third person. The video was posted by a bot account on X linked to Storm-1516, which posed as an American named "Scott Golberg" on Election Day with the caption, "Unsuspecting Trump voter got attacked by two men at polling station in WI! One of them wearing Harris hoodie". The video was subsequently amplified by real and fake accounts, garnering hundreds of thousands of views. The Wisconsin Election Commission confirmed that the incident did not take place.

Screenshot of two Russian accounts linked to Storm-1516 amplifying fabricated video.

Source: Darren Linvill

Foreign cybercriminals use Wyoming shell companies for global hacking campaigns on media companies

State: Wyoming

Threat Actor: Unknown / Various foreign cybercriminals

Date: September - December 2023

Objectives: Dissuade from Acting (silence) and Undermine (smear)

Select Channels & Affordances: N/A

Tactics & Techniques: Drive Online Harms (control information environment through offensive cyberspace operations)

Foreign cybercriminals reportedly used Wyoming shell companies for global hacking operations targeting media companies by helping them pass their internet traffic off as originating from within the United States. According to investigations by Qurium, a nonprofit that does digital defense work for news organizations, at least three major cyberattacks between September and December 2023 were traced to limited liability companies in Wyoming. In August, cybercriminals used an IP address linked to Aliat, a company based in Sheridan, Wyoming, to shut down the Somali Journalist Syndicate's website and email accounts days before one of Syndicate's anti-corruption journalists was abducted by Somali authorities. In another incident, a distributed denial of service, or DDoS, attack knocked out the website of the Vienna-based International Press Institute for ten days, shortly after it had published a report on cyber threats to Hungarian media freedom. The attack was traced to a Wyoming web hosting company called HostCram.

Conclusion

While some of the examples in this report are starker than others, not a single US state remains untouched by foreign information operations. Foreign actors may focus disproportionately on swing states during national elections, but our research reveals that states big and small, red and blue, have all been targeted by foreign threat actors—and often without any direct connection to US elections. We believe that advances in AI, in particular, will allow for even more targeted foreign state campaigns at the local level.

It is well established that foreign actors exploit domestic vulnerabilities, including political and social cleavages, to exacerbate discord in the United States. But domestic challenges should not provide an excuse for inaction. Americans need more leaders, especially trusted voices in state and local communities, engaging their communities on information manipulation and how foreign adversaries' targeting of citizens affects US national security. As many of our cases illustrate, every citizen is a potential entry point for an adversary—and Americans need to act like it.

What Americans say or believe is not the focus of this report. The principle of free speech should remain unimpeded. Rather, it is about understanding the tactics, techniques, and objectives of US adversaries, who have a vested interest in surreptitiously putting their thumb on the scales of organic domestic discourse to fuel polarization and destabilize American institutions and society. Arming citizens with this knowledge, we believe, can make all Americans less prone to these operations going forward.

About the Alliance for Securing Democracy at GMF

The Alliance for Securing Democracy (ASD) at the German Marshall Fund of the United States is a non-partisan initiative that exposes, analyzes, and develops strategies to counter foreign information manipulation and interference in democracies. ASD leverages its data and expertise to provide sharp analysis and actionable recommendations to counter these threats to relevant public and private sector actors. With staff in Washington, DC and Brussels, ASD translates lessons learned from countries' experiences addressing foreign information manipulation and interference for key stakeholders on both sides of the Atlantic—and, increasingly, around the world. ASD also aims to be a force multiplier, partnering with likeminded organizations to strengthen resilience among democracy's most crucial asset—the citizenry

Acknowledgment

The authors would like to acknowledge Louis Savoia, Annika Sharp, and James Conway for providing research support for this report.

Author Bios

Krystyna Sikora is a research assistant for ASD at GMF, where she spearheads research on election integrity and information manipulation. She received an MA in Eurasian, Russian, and East European studies from Georgetown University, where she centered her studies on right-wing populism, the information space, and democratic decline in Central and Eastern Europe. Prior to joining ASD, Krystyna played professional soccer in Poland for two years.

Bret Schafer is a senior fellow at ASD at GMF, where he leads ASD's information manipulation team. Bret is the creator and manager of Hamilton 2.0, an online open-source dashboard tracking the outputs of Russian, Chinese, and Iranian state media outlets, diplomats, and government officials. As an expert in computational propaganda, state-backed information operations, and tech regulation, he has spoken at conferences around the globe and advised numerous governments and international organizations. Prior to joining ASD, Bret spent more than 10 years in the television and film industry.

Ankara • Belgrade • Berlin • Brussels • Bucharest

Paris • Warsaw • Washington, DC

gmfus.org