

# Meta disrupted China-based propaganda machine before it reached many Americans



## reader comments

49 with 37 posters participating

## Share this story

China's ability to influence American politics by manipulating social media platforms has been a topic of much scrutiny ahead of the midterm elections, and this week has marked some progress toward mitigating risks on some of the most popular US platforms.

US President Joe Biden is currently working on a deal with China-based TikTok—often regarded as a significant threat to

US national security—with the one goal of blocking potential propaganda or misinformation campaigns. Now today, Meta, owner of Facebook and Instagram, shared a report detailing the steps it took to remove the first “Chinese-origin influence operation” that Meta has identified attempting “to target US domestic politics ahead of the 2022 midterms.”

In the press release, Meta Global Threat Intelligence Lead Ben Nimmo joined Meta Director of Threat Disruption David Agranovich in describing the operation as initiated by a “small network.” They said that between fall 2021 and September 2022, there were four “largely separate and short-lived” efforts launched by clusters of “around half a dozen” China-based accounts, which targeted both US-based conservatives and liberals using platforms like Facebook, Instagram, and Twitter.

In total, Meta removed “81 Facebook accounts, eight pages, one group, and two accounts on Instagram.” Meta estimated approximately 250 accounts joined the group, 20 accounts followed one or more Pages, and fewer than 10 accounts followed one or both Instagram accounts.

“This was the first Chinese network we disrupted that focused on US domestic politics ahead of the midterm elections,” the press release said. Previously, Meta had only disrupted Chinese networks that were working to influence opinions on US politics held by audiences outside the US.

When Meta monitors this type of activity, which it calls “coordinated inauthentic behavior,” it says in its report that it’s looking for fake accounts intentionally manipulating public debate. The bad actors do this by coordinating actions of multiple fake accounts “to mislead others about who they are and what they are doing.”

Advertisement

Meta policy dictates that this type of moderation is about

monitoring account behavior, not the content of posts. Examples in the report include fake accounts posting memes targeting the left by alleging that the National Rifle Association of America paid off Senator Marco Rubio (R-Fla.) and the right by depicting a tentacled Biden gripping the world bearing nukes and machine guns. What gets an account removed is not, Meta said, “what they post or whether they’re foreign or domestic,” but whether the network would collapse without the fake accounts propping it up.

A Meta spokesperson told Ars that it focuses on “violating deceptive behavior, not content,” to take down covert influence operations because “these networks typically post content that isn’t provably false, but they rather aim to mislead people about who’s behind it and what they are doing.”

In the press release, Nimmo and Agranovich summed up the extent of the Chinese network’s reach and how well Meta worked to detect its deceptive behaviors, writing: “Few people engaged with it, and some of those who did called it out as fake. Our automated systems took down a number of accounts and Facebook Pages for various Community Standards violations, including impersonation and inauthenticity.”

## **Other threats detected**

In the same report, Meta described a takedown of a much larger instance of “coordinated inauthentic behavior” originating from Russia.

Described as the largest Russian network of its kind that Meta has “disrupted since the war in Ukraine began,” this second operation targeted users based in “primarily Germany, France, Italy, Ukraine, and the UK.” Its online presence spanned 1,633 Facebook accounts, 703 Facebook pages, one Facebook group, and 29 accounts on Instagram.” The reach was limited to 4,000 accounts following at least one page, fewer than 10 accounts joining the group, and 1,500 accounts following at least one

Instagram account. The operation also invested \$105,000 in Facebook and Instagram ads, “paid primarily in US dollars and euros.”

The Russian network began operating in May, Meta reported, by launching more than 60 websites “carefully impersonating legitimate websites of news organizations in Europe,” such as Spiegel and The Guardian. It’s concerning because of the attention to detail mimicked authoritative news sites and translated articles into different languages. The operation relied on Facebook, Instagram, petitions on Change.org, Twitter, YouTube, and other social networks in its attempt to spread its fraudulent information.

#### Advertisement

German investigative journalists tipped off Meta to the problem, and when Meta tried to block domains, the network “attempted to set up new websites, suggesting persistence and continuous investment in this activity across the Internet.”

“This is the largest and most complex Russian-origin operation that we’ve disrupted since the beginning of the war in Ukraine,” Nimmo and Agranovich wrote in the press release. “It presented an unusual combination of sophistication and brute force. The spoofed websites and the use of many languages demanded both technical and linguistic investment.”

But while Meta considered the Russian network “unusual,” a report from the Stanford Internet Observatory (SIO) Cyber Policy Center released last month described the majority of these tactics as common.

For their report, SIO evaluated Meta and Twitter data covering a period of five years of pro-Western covert influence operations, which the platforms had already jointly removed.

To complete its analysis, SIO worked with the social media analytics firm Graphika to identify “an interconnected web of accounts on Twitter, Facebook, Instagram, and five other

social media platforms that used deceptive tactics to promote pro-Western narratives in the Middle East and Central Asia,” as well as narratives that heavily criticized Russia, China, and Iran.

Twitter’s dataset “covered 299,566 tweets by 146 accounts between March 2012 and February 2022,” but Meta’s was limited to “39 Facebook profiles, 16 pages, two groups, and 26 Instagram accounts active from 2017 to July 2022.” Combining the datasets left SIO with five years’ worth of cross-platform activities from the influence operations to analyze.

Hoping to better understand “how different actors use inauthentic practices to conduct online influence operations,” SIO found that these operations have a limited range of tactics, employing the same—mostly unsuccessful strategies—over and over.

“The assets identified by Twitter and Meta created fake personas with GAN-generated faces, posed as independent media outlets, leveraged memes and short-form videos, attempted to start hashtag campaigns, and launched online petitions: all tactics observed in past operations by other actors,” SIO’s report said.

In Meta’s most recent report, tactics included relying on “crude ads,” generating fake profiles, impersonating journalists, leveraging memes, launching online petitions, and posting comments on influential accounts for maximum visibility.

<https://arstechnica.com/?p=1885001>