NOVEMBER 2022

DETAILED REPORT

Quarterly Adversarial Threat Report

Meta

TABLE OF CONTENTS

PURPOSE OF THIS REPORT

Over the past five years, we've shared our findings about coordinated inauthentic behavior (CIB) we detect and remove from our platforms. As part of our quarterly adversarial threat reports, we're sharing information about the networks we take down to make it easier for people to see progress we're making in one place. We welcome ideas from the security community to help us make these reports more informative and we'll adjust as we learn from feedback.

For a quantitative view into our Community Standards' enforcement in the third quarter of 2022, including content-based actions we've taken at scale and our broader integrity work, please visit our Transparency Center.

WHAT IS COORDINATED INAUTHENTIC BEHAVIOR (CIB)?

We view CIB as coordinated efforts to manipulate public debate for a strategic goal, in which fake accounts are central to the operation. In each case, people coordinate with one another and use fake accounts to mislead others about who they are and what they are doing. When we investigate and remove these operations, we focus on behavior rather than content — no matter who's behind them, what they post or whether they're foreign or domestic.

Continuous CIB enforcement: We monitor for efforts to come back by the networks we previously removed. Using both automated and manual detection, we continuously remove accounts and Pages connected to networks we took down in the past.

SUMMARY OF OUR FINDINGS

- Our third quarterly threat report provides a view into three covert influence operations we investigated and removed for violating our policy against CIB.
- The first network originated in the United States and was linked to individuals associated with the US military. We shared our findings with independent researchers who then reported on this network on August 24, 2022.
- The second operation originated in China and targeted the United States, the Czech Republic and, to a lesser extent, Chinese- and French-speaking audiences around the world. (Originally reported on September 27, 2022)
- The last network originated in Russia and targeted primarily Germany, and also France, Italy, Ukraine and the United Kingdom. (Originally reported on September 27, 2022) .

01

United States

We removed 39 Facebook accounts, 16 Pages, two Groups and 26 accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in the United States and focused on a number of countries including Afghanistan, Algeria, Iran, Iraq, Kazakhstan, Kyrgyzstan, Russia, Somalia, Syria, Tajikistan, Uzbekistan and Yemen.

We found several clusters of activity that relied on fake accounts — some of which were detected and disabled by our automated systems prior to our investigation — to post content, drive people to off-platform domains and manage Groups and Pages. These regional clusters were focused on Iran and the Gulf, Central Asia, and the Middle East and North Africa. Typically, each cluster posted about particular themes, including sports and culture in a particular country; cooperation with the United States, including military cooperation; and criticism of Iran, China, or Russia.

The people behind this network posed as locals in the countries they targeted. Some of these accounts used profile photos likely generated using machine learning techniques like GAN (generative adversarial networks). Some of the Pages operated small media brands — with their distinct logos and visual style — and had presence across different internet services including Twitter, YouTube, Telegram, the Russian VKontakte and Odnoklassniki, blogs and websites. They posted videos, articles, photos and memes about the country they focused on. When these brands ran the same image or meme, they would each superimpose its own logo on it, likely to make the content appear more unique and credible.

This network posted primarily during US business hours (EST) rather than during work hours in the countries they targeted. The majority of this operation's posts had little to no engagement from authentic communities.

The people behind this activity posted primarily in Arabic, Farsi and Russian about news and current events, including terrorism concerns and praise of the US military, as well as content about the COVID-19 pandemic — some of which we removed for violating our misinformation policy. This operation also shared posts criticizing Iran, China and Russia, including Russia's invasion of Ukraine,

China's treatment of the Uyghur people, Iran's influence in the Middle East, and the support of the Taliban regime in Afghanistan by Russia and China.

We found this activity as part of our internal investigation into suspected coordinated inauthentic behavior in the region. We shared information about this network with independent researchers at Graphika and the Stanford Internet Observatory, who have published their findings about this network's activity across the internet on August 24, 2022. Although the people behind this operation attempted to conceal their identities and coordination, our investigation found links to individuals associated with the US military.

- *Presence on Facebook and Instagram:* 39 Facebook accounts, 16 Pages, two Groups and 26 accounts on Instagram.
- *Followers:* About 22,000 accounts followed one or more of these Pages, about 400 accounts joined at least one of these Groups and around 12,000 accounts followed one or more of these Instagram accounts.
- *Advertising:* About $2,500 in spending for ads on Facebook paid for in US dollars and British pounds.

02

China

Originally reported on September 27, 2022

We took down 81 Facebook accounts, eight Pages, one Group and two accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in China and targeted the United States, the Czech Republic and, to a lesser extent, Chinese- and French-speaking audiences around the world.

It included four, largely separate and short-lived efforts, each focused on a particular audience at different times between the Fall of 2021 and 2022. In the United States, they targeted people on both sides of the political spectrum. In Czechia, this activity focused on criticizing the state's support of Ukraine, its impact on the Czech economy, and calling for the government to avoid antagonizing China. Each cluster of accounts — around half a dozen each — posted content at low volumes during working hours in China rather than when their target audiences would typically be awake. Only a 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 Pages for various community standards violations, including impersonation and inauthenticity.

This operation ran across multiple internet services, including Facebook, Instagram, Twitter and two Czech petition platforms. This was the first Chinese network we disrupted that focused on US domestic politics ahead of the midterm elections, as well as Czechia's foreign policy toward China and Ukraine. Chinese influence operations that we've disrupted before typically focused on criticizing the United States to international audiences, rather than primarily targeting domestic audiences in the US. A network that we took down in 2020 included a very limited effort to post about US politics, but primarily focused on the Philippines and Southeast Asia.

- *Presence on Facebook and Instagram:* 81 Facebook accounts, eight Pages, one Group and two accounts on Instagram.

- *Followers:* About 20 accounts followed one or more of these Pages, around 250 accounts joined this Group and less than 100 accounts followed one or more of these Instagram accounts.

See our prior reporting with detailed threat research on this operation, including threat indicators, here.

03

Russia

Originally reported on September 27, 2022

We took down 1,633 accounts, 703 Pages, one Group and 29 accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in Russia and targeted primarily Germany, and also France, Italy, Ukraine and the United Kingdom.

The operation began in May of this year and centered around a sprawling network of over 60 websites carefully impersonating legitimate news organizations in Europe, including Spiegel, The Guardian, Bild and ANSA. There, they would post original articles that criticized Ukraine and Ukrainian refugees, praised Russia and argued that Western sanctions on Russia would backfire. They would then promote these articles and also original memes and YouTube videos across many internet services, including Facebook, Instagram, Telegram, Twitter, petitions websites Change.org and Avaaz, and even LiveJournal. Throughout our investigation, as we blocked this operation's domains, they attempted to set up new websites, suggesting persistence and continuous investment in this activity. In fact, we continued to update our original report with new domains this operation keeps creating online. They operated primarily in German, English, French, Italian, Spanish, Russian and Ukrainian. On a few occasions, the operation's content was amplified by Russian embassies in Europe and Asia.

We began our investigation after reviewing public reporting into a portion of this activity by investigative journalists in Germany. The researchers at the Digital Forensic Research Lab also provided insights into a part of this network, and we've shared our findings with them to enable further research into the broader operation.

This is the largest and most complex Russian-origin operation that we've disrupted since the beginning of the war in Ukraine. 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. The amplification on social media, on the other hand, relied primarily on crude ads and fake accounts. In fact, on our platforms, the majority of the accounts, Pages and ads were detected and removed by our automated systems before we even began our investigation.

Together, these two approaches worked as an attempted smash-and-grab against the information environment, rather than a serious effort to occupy it long-term.

To support further research into this and similar cross-internet activities, we are including a list of domains, petitions and Telegram channels that we have assessed to be connected to the operation. We look forward to further discoveries from the research community.

Update as of December 15, 2022: Our investigations linked this network to two companies in Russia: Structura National Technologies, an information technology firm, and Social Design Agency (Агентство Социального Проектирования), a marketing and political consulting firm.

- *Presence on Facebook and Instagram:* 1,633 accounts, 703 Pages, one Group and 29 accounts on Instagram.
- *Followers:* About 4,000 accounts followed one or more of these Pages, less than 10 accounts joined this Group and about 1,500 accounts followed one or more of these Instagram accounts.
- *Advertising:* Around $105,000 in spending for ads on Facebook and Instagram, paid for primarily in US dollars and euros.

See our prior reporting with detailed threat research on this operation, including threat indicators, here.