MAY 2025

FIRST QUARTER

Adversarial Threat Report

Meta

TABLE OF CONTENTS

PURPOSE OF THIS REPORT

Our public threat reporting began in 2017 when we first shared our findings about coordinated inauthentic behavior (CIB) by a Russian covert influence operation linked to the Internet Research Agency (IRA). Since then, we have evolved our capability to respond to a wider range of adversarial behaviors as global threats have continued to evolve. To provide a more comprehensive view into the risks we tackle, we've also expanded our threat reports to include insights into other threats, as part of our quarterly reporting. In addition, we're also publishing threat indicators to contribute to the security community's efforts to detect and counter malicious activity across the internet (see Appendix).

We expect the make-up of these reports to change from quarter to quarter in response to the changes we see in the global threat environment. This report is not meant to reflect the entirety of our security enforcements, but to share notable trends and investigations to help inform the security community's understanding of the evolving threats we see. We welcome ideas from our peers to help make these reports more informative.

For a quantitative view into our enforcement of our Community Standards, including content-based actions we've taken at scale and our broader integrity work, please visit Meta's Transparency Center here: https://transparency.fb.com/data/.

What is Coordinated Inauthentic Behavior or 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, not content — no matter what they post or whether they're foreign or domestic.

Continuous CIB enforcement: We monitor for efforts to come back by 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.

EXECUTIVE SUMMARY

In this report, we're sharing threat research into three covert influence operations we disrupted in Q1 of 2025 in China, Iran, and Romania. We detected and removed these campaigns before they were able to build authentic audiences on our apps.

- **China**: We removed a network that originated in China that targeted Myanmar, Taiwan, and Japan. We detected and took it down as a result of our internal investigation into suspected CIB activity in the region, before the operators were able to build authentic audiences on our apps. Although the people behind it attempted to conceal their identity and coordination, our investigation found links to two separate China-based influence operations we had previously removed and reported in September 2022 and February 2024.
- **Iran**: We removed a network that originated in Iran and targeted Azeri-speaking audiences in Azerbaijan and Turkey across multiple internet services including ours, X (formerly Twitter), YouTube, and on their own websites. We began our investigation into this network after reviewing information about a portion of its activity shared with us by analysts at Google Threat Intelligence Group. We removed this activity before the operators were able to build authentic audiences on our apps, and we also found links between this operation and the STORM-2035 activity reported on by OpenAI and Microsoft in August 2024.
- **Romania**: We removed a network that originated in and targeted Romania across multiple internet services including ours, YouTube, X and TikTok. We detected and removed this activity as a result of our internal investigation into suspected coordinated inauthentic behavior in the region, before this operation was able to build an audience among authentic communities on our apps.

01

China

We removed 157 Facebook accounts, 19 Pages, one Group, and 17 accounts on Instagram for violating our coordinated inauthentic behavior policy. This network originated in China, and targeted Myanmar, Taiwan, and Japan. We disrupted it before it was able to build authentic audiences on our apps.

The people behind this activity used fake accounts – many of which were detected by our automated systems – to post content, manage Pages, and reach out to others. This operation included three separate clusters of accounts where each targeted a particular country while posing as locals. Some of these accounts used profile photos likely created using artificial intelligence. The same group also operated a so-called account farm creating further fake accounts which we took action against separately.

These three clusters reposted other people's and their own content in English, Burmese, Mandarin, and Japanese about news and current events in each country they targeted. In Myanmar, they posted about the need to end the ongoing conflict, criticized the civil resistance movements and shared supportive commentary about the military junta. In Japan, the campaign criticized Japan's government and its military ties with the US. In Taiwan, they posted claims that Taiwanese politicians and military leaders are corrupt, and ran Pages claiming to display posts submitted anonymously – in a likely attempt to create the impression of an authentic discourse.

We found this network as a result of our internal investigation into suspected CIB activity in the region. Although the people behind it attempted to conceal their identity and coordination, our investigation found links to two past China-based influence operations we had removed and reported in September 2022 and February 2024.

- Presence on Facebook and Instagram: 157 Facebook accounts, 19 Pages, 1 Group, and 17 accounts on Instagram.
- Followers: About 7,800 accounts followed one or more of these Pages, around 25 users joined this Group, and about 700 users followed one or more of these Instagram accounts.

02

Iran

We removed 17 accounts on Facebook, 22 FB Pages and 21 accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in Iran and targeted Azeri-speaking audiences in Azerbaijan and Turkey across multiple internet services including ours, X (formerly Twitter), YouTube, and on their own websites. We removed this activity before the operators were able to build authentic audiences on our apps.

The people behind this activity used fake accounts – some of which were detected and disabled by our automated systems prior to our investigation – to post content, including in Groups, manage Pages, and to comment on the network's own content – likely to make it appear more popular than it was. Many of these accounts posed as female journalists and pro-Palestine activists. The operation also used popular hashtags like #palestine, #gaza, #starbucks, #instagram in their posts, as part of its spammy tactics in an attempt to insert themselves in the existing public discourse.

The operators posted in Azeri about news and current events, including the Paris Olympics, Israel's 2024 pager attacks, boycott of American brands, and criticisms of the US, President Biden and Israel's actions in Gaza.

We found this network after reviewing information about a portion of its activity shared with us by analysts at Google Threat Intelligence Group. We also found links between this operation and the STORM-2035 activity reported on by OpenAI and Microsoft in August 2024.

- *Presence on Facebook and Instagram:* 17 accounts on Facebook, 22 Pages, and 21 Instagram accounts.
- *Followers:* About 44,000 accounts followed one or more of these Pages, and about 63,000 accounts followed one or more of these Instagram accounts.
- Ad spend: About $70 in spending for ads, paid for primarily in US and Canadian dollars.

03

Romania

We took action against 658 accounts on Facebook, 14 Pages, and two accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in and targeted Romania across multiple internet services including ours, YouTube, X and TikTok. We detected and removed this activity before this operation was able to build an audience among authentic communities on our apps.

The people behind this activity used fake accounts – some of which were detected and disabled by our automated systems prior to our investigation – to manage Pages, drive people to off-platform websites, and comment on posts by politicians and news entities. The majority of these comments received no engagement from authentic audiences. These accounts posed as locals in Romania posting about sports, travel, or local news and had a corresponding presence on YouTube, X, and TikTok, likely to backstop their fictitious personas and entities across the internet in an attempt to make them appear more credible. This campaign showed consistent operational security (OpSec) to conceal its origin and coordination, including by relying on proxy IP infrastructure. The people behind this effort posted primarily in Romanian about news and current events, including elections in Romania.

We found this network as a result of our internal investigation into suspected coordinated inauthentic behavior in the region.

- *Presence on Facebook and Instagram:* 658 accounts on Facebook, 14 Pages, 2 accounts on Instagram.
- *Followers:* About 18,300 accounts followed one or more of these Pages and around 40 accounts followed one or more of these Instagram accounts.
- Ad spend: About $177,000 in spending for ads, paid for primarily in US dollars.

Appendix: Threat indicators

The following section details unique threat indicators that we assess to be associated with the malicious networks we disrupted and described in this report. To help the broader research community to study and protect people across different internet services, we've collated and organized these indicators according to the Online Operations Kill Chain framework, which we use to analyze many sorts of malicious online operations, identify the earliest opportunities to disrupt them, and share information across investigative teams. The kill chain describes the sequence of steps that threat actors go through to establish a presence across the internet, disguise their operations, engage with potential audiences, and respond to takedowns.

We're sharing these threat indicators to enable further research by the open-source community into any related activity across the web (GitHub). This section includes the latest threat indicators and is not meant to provide a full cross-internet, historic view into these operations. It's important to note that, in our assessment, the mere sharing of these operations' links or engaging with them by online users would be insufficient to attribute accounts to a given campaign without corroborating evidence.

CHINA-BASED CIB NETWORK

Tactic	Threat indicator
Acquiring Assets	
Acquiring Facebook accounts	157 accounts
Acquiring Facebook Pages	19 Pages
Acquiring Instagram accounts	17 accounts
Acquiring Facebook Groups	1 group
Acquiring YouTube channels	*www.youtube[.]com/watch?v=FXCzsTm4GHU&t=2s*
Acquiring TikTok accounts	*www.tiktok[.]com/@user8101771158572*

Disguising Assets	
Adopting visual disguise	Using profile photos likely generated using artificial intelligence such as Generative Adversarial Networks (GAN)
Posing as non-existent person	We found three separate clusters of accounts where each targeted a particular country while posing as locals.
Indiscriminate Engagement	
Amplifying with likely fake accounts on Facebook, Instagram	The people behind this activity used fake accounts – many of which were detected by our automated systems – to post content, manage Pages, and reach out to others.
Targeted Engagement	
Engaging with users outside the operation	About 7,800 accounts followed one or more of these Pages
	Around 25 users joined the Group
	About 700 users followed one or more of these Instagram accounts
Engaging with specific audience	These three clusters reposted other people's and their own content in English, Burmese, Mandarin, and Japanese about news and current events in each country they targeted.
Posting about individuals or institutions	In Myanmar, they posted about the need to end the ongoing conflict, criticized the civil resistance movements and shared supportive commentary about the military junta
	In Japan, the campaign criticized Japan's government and its military ties with the US.
	In Taiwan, they posted claims that Taiwanese politicians and military leaders are corrupt.

IRAN-BASED CIB NETWORK

Tactic	Threat indicator
Acquiring Assets	
Acquiring Facebook accounts	17 accounts
Acquiring Facebook Pages	22 Pages
Acquiring Instagram accounts	21 accounts
Acquiring domains to support influence operations	israelboycottvoice[.]com
	palestinesupporter[.]com
Acquiring X / Twitter accounts	twitter[.]com/BoycottVoice3
Disguising Assets	
Posing as fictional journalists & activists	Many of these accounts posed as female journalists and pro-Palestine activists
Indiscriminate Engagement	
Amplifying with likely fake accounts on Facebook, Instagram	The people behind this activity used fake accounts – some of which were detected and disabled by our automated systems prior to our investigation – to post content, including in Groups, manage Pages, and to comment on the network's own content – likely to make it appear more popular than it was.
Targeted Engagement	
Running Ads	About $70 in spending for ads, paid for primarily in US and Canadian dollars.
Engaging with users outside the operation	About 44,000 accounts followed one or more of these Pages
	about 63,000 accounts followed one or more of these Instagram accounts

Engaging with specific audience	The operation used popular hashtags like #palestine, #gaza, #starbucks, #instagram in their posts, as part of its spammy tactics in an attempt to insert themselves in the existing public discourse.
Posting about individuals or institutions	The operators posted in Azeri about news and current events, including the Paris Olympics, Israel's 2024 pager attacks, boycott of American brands, and criticisms of the US, President Biden and Israel's actions in Gaza.

ROMANIA-BASED CIB NETWORK

Tactic	Threat indicator
Acquiring Assets	
Acquiring Facebook accounts	658 accounts
Acquiring Facebook Pages	14 Pages
Acquiring Instagram accounts	2 accounts
Acquiring X / Twitter accounts	x[.]com/popa_mariannn
Acquiring X / Twitter accounts	x[.]com/ionitaeva509
Acquiring X / Twitter accounts	x[.]com/nicolescuanas31
Acquiring X / Twitter accounts	x[.]com/DariusMindru
Acquiring X / Twitter accounts	x[.]com/nicolasstoica98
Acquiring X / Twitter accounts	x[.]com/campau_sorin
Acquiring YouTube channels	www.youtube[.]com/@M%C4%83tu%C8%99adela%C8%9Bar%C4%83-r4y
Acquiring YouTube channels	www.youtube[.]com/@Prost%C4%83nacul-x6z
Acquiring TikTok accounts	www.tiktok[.]com/@emilmitreaa
Acquiring TikTok accounts	www.tiktok[.]com/@bucursofiaa

Acquiring TikTok accounts	www.tiktok[.]com/@dariusvictoria
Acquiring TikTok accounts	www.tiktok[.]com/@nicolasstoica50
Acquiring TikTok accounts	www.tiktok[.]com/@campausorin
Disguising Assets	
Posing as non-existent person	This operation's accounts posed as locals in Romania posting about sports, travel or local news.
Backstopping	These accounts posed as locals in Romania posting about sports, travel, or local news and had a corresponding presence on YouTube, X, and TikTok, likely to backstop their fictitious personas and entities across the internet in an attempt to make them appear more credible.
Evading Detection	
Obfuscating infrastructure	This campaign showed consistent operational security (OpSec) aimed to conceal its origin and coordination, including by relying on proxy IP infrastructure.
Indiscriminate Engagement	
Amplifying with likely fake accounts on Facebook	The people behind this activity used fake accounts to manage Pages, drive people to off-platform websites, and comment on posts by politicians and news entities. The majority of these comments received no engagement from authentic audiences.
Targeted Engagement	
Running Ads	About $177,000 in spending for ads, paid for primarily in US dollars.
Engaging with users outside the operation	About 18,300 accounts followed one or more of these Pages.
Engaging with users outside the operation	Around 35 accounts followed one or more of these Instagram accounts.