FEBRUARY 2025

FOURTH QUARTER

Adversarial Threat Report

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. See the Doppelganger section for details on our approach to persistent threats.

EXECUTIVE SUMMARY

In this report, we're sharing threat research into three covert influence operations we disrupted in Q4 of 2024 in Benin, Ghana and China. We detected and removed these campaigns before they were able to build authentic audiences on our apps. We're also including an update on the most persistent Russian covert influence operation known as Doppelganger.

- **Benin**: We removed 16 Facebook accounts and six Pages in Benin that targeted primarily France and to a much lesser extent the United States, as part of a broader operation across the internet, including on our apps, Telegram, X, and their own website. We found this campaign as a result of our internal investigation. Our investigation benefited from public reporting about some of this activity. Our investigation found links to Digited Consulting, a firm in Benin. This firm is now banned from our apps and we sent it a cease and desist letter.

- **Ghana**: We removed 42 accounts on Facebook, one Page, and 33 accounts on Instagram in Ghana that targeted domestic audiences in that country across the internet including our apps, X, YouTube, TikTok, and on their own website. We found this network after reviewing information shared with us by our peers at OpenAI about a small portion of this activity, and removed it before the operators were able to build authentic audiences on our apps. Our investigation found links to the UAE marketing firm DigitSol with an office in Ghana.

- **China**: We removed 18 Facebook accounts, two Pages, four Groups and five accounts on Instagram from China that targeted the Tibetan diaspora primarily in Nepal, India and Bhutan across multiple services including ours, X, and Blogspot. We found this activity as a result of our internal investigation into suspected recidivist activity linked to the network we removed and reported in Q3 2023. We took down this network before its operators were able to build an audience among authentic communities on our apps.

- **Russia**: As part of our ongoing reporting on Doppelganger, a cross-internet influence operation from Russia, we're sharing our latest research into this persistent campaign. Our insights include: Doppelganger's shift in geographic targeting away from the US, Ukraine, and Poland; continued pause in sharing of links to this campaign's off-platform websites; narrative focus on portraying the US as an unreliable partner to France, Germany, and Israel; and continued low efficacy of this operation's efforts on our apps with most attempts to acquire fake accounts or run ads being quickly detected and blocked.

01

Benin

We removed 16 Facebook accounts and six Pages for violating our coordinated inauthentic behavior policy. This network originated in Benin, and targeted primarily France and to a much smaller extent the US. We disrupted it before it was able to build authentic audiences on our apps.

First, the people behind this operation created Pages which posed as French and posted about politics in France, but were run by authentic users in Benin. In addition they maintained efforts on Telegram, X (formerly Twitter) and their own website. We quickly took down this activity on our apps.

In response to enforcement, they changed tactics. Instead of using authentic accounts, the operators created a network of fake and compromised accounts, and used TOR and proxy IP infrastructure to conceal their origin and appear to be in France. Our automated systems and expert investigators continued to detect and take them down on a rolling basis. This campaign used profile photos likely generated using AI, used text obfuscation techniques to try to evade automated detection, and posted apparent GenAI images. The operators also deployed stronger operational security (OpSec) to conceal their activity.

This effort targeted primarily France with posts in French about news and politics, including criticism of President Macron and NATO; supportive commentary about Marine Le Pen and her party; and calls for reduced support for Ukraine. In the US, they used one Page in an attempt to amplify an off-platform website – which mimicked the Harris campaign site – through a handful of ads. Our automated detection and investigators stopped them. The Page had one follower when we removed it. While the website appeared to look like the real campaign site, its *Issues* page contained fictitious claims about the campaign's positions including on the aid to Ukraine. We blocked the website from being shared on our apps.

We found this campaign as part of our internal investigation into suspected coordinated inauthentic behavior. Our investigation benefited from public reporting about some of this activity. Although the people behind it attempted to conceal their identity and coordination, our investigation found links to Digited Consulting, a firm in Benin, likely working on behalf of an unknown client. This firm is now banned from our apps and we sent it a cease and desist letter.

- *Presence on Facebook and Instagram:* 16 Facebook accounts and 6 Pages.
- *Followers*: About 18,000 accounts followed one or more of these Pages.
- *Ad spend:* About $1,300 in spending for ads, paid for mostly in US and Canadian dollars.

02

Ghana

We removed 42 accounts on Facebook, one Page, and 33 accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated primarily in Ghana and targeted audiences in that country across multiple internet services including ours, X (formerly Twitter), YouTube, TikTok, and on their own website.

The people behind this activity used fake accounts – many of which were detected and disabled by our automated systems prior to our investigation – to manage Pages and comment on their own content. This operation centered around a fictitious youth movement *Empowering Ghana* (EG) which had its own website and presence on multiple internet platforms. Some of the fake accounts used profile photos likely generated using artificial intelligence and posed as fictitious journalists and activists across many apps and on the EG website. The operators used fake accounts to comment on this fictitious movement, likely to make it appear to have local support. According to OpenAI's report, these comments were created using GenAI. They received no to minimal engagement among authentic audiences on our apps.

The people behind this effort posted primarily in English about politics in Ghana, including supportive commentary about the former Vice President Bawumia who lost in the latest Presidential election. We removed this activity in advance of the December 2024 election in Ghana, before the operators were able to build authentic audiences on our apps.

We found this network after reviewing information shared with us by our peers at OpenAI. Although the people behind it attempted to conceal their identity and coordination, our investigation found links to the UAE marketing firm DigitSol with an office in Ghana.

- *Presence on Facebook and Instagram:* 42 Facebook accounts, 1 Page, and 33 accounts on Instagram.
- *Followers:* About 38,000 accounts followed one or more of these Pages, and about 880,000 accounts followed one or more of these Instagram accounts. The vast majority of Instagram followers were outside of Ghana, suggesting the use of fake engagement tactics to make this operation appear more successful than it actually was.
- Ad spend: About $10,200 in spending for ads, paid for mostly in US dollars.

03

China

We removed 18 Facebook accounts, two Pages, four Groups and five accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in China and targeted the Tibetan diaspora primarily in Nepal, India and Bhutan across multiple services including ours, X (formerly Twitter) and Blogspot.

The individuals behind this activity used fake accounts – many of which were detected and disabled by our automated systems prior to our investigation – to manage Pages, post and amplify other people's content. They used proxy IPs to conceal their origin and appear to be coming from India, Bhutan or Nepal. The operation created a handful of fictitious personas, including one posing as a journalist in the Arunachal Pradesh region of India. Most of the accounts posed as Tibetan expats, showed little complexity and were used primarily to reshare content from real people.

The network posted mainly in English and Tibetan about news related to Tibet and its politics, including criticism of exiled Tibetan leader the Dalai Lama, conspiracies about his travel and health, and claims that the United States is using him as a lever against China. They also posted supportive commentary about Ogyen Trinley Dorje, a self-exiled Tibetan buddhist leader, and the need to normalize relations between Tibet and China. This campaign frequently amplified anti-Dalai Lama posts by authentic voices including sharing links to websites like Storify News, Dakini Translations and Publications, and a Change dot org petition in support of Ogyen Trinley Dorje. We also saw examples of posting on both sides of the political debate at once where one fake account would post in support of the Dalai Lama and another would criticize him.

We found this activity as a result of our internal investigation into suspected recidivist activity linked to the network we removed and reported in Q3 2023. We removed this operation before it was able to build an audience among authentic communities.

- *Presence on Facebook and Instagram:* 18 Facebook accounts, 2 Pages, 4 Groups and 5 Instagram accounts.
- *Followers:* About 2,400 accounts followed one or more of these Pages, about 120 accounts joined one or more of these Groups, and about 100 accounts followed one or more of these Instagram accounts.

04

Russia

DOPPELGANGER'S ATTEMPTS TO STAY AFLOAT ACROSS THE INTERNET

As part of our ongoing reporting on Doppelganger, a cross-internet influence operation from Russia, we're sharing our **10th** update in nearly **2.5** years that includes our latest research into this malicious activity.[1] Our industry peers and researchers can find our repository of 6,000+ threat indicators related to this campaign so they can investigate and take action as appropriate.

WHAT IS DOPPELGANGER?

In 2022, we were the first technology company to publicly report on Doppelganger, an operation centered around a network of websites spoofing legitimate news outlets. The EU Disinfo Lab and the Digital Forensic Research Lab published their research at the same time.

Attribution: Doppelganger appears to be the work of multiple groups of operators. In December 2022, we were the first to publicly attribute it to two companies in Russia – Structura National Technology and Social Design Agency. They were sanctioned by the EU in 2023 and by the US Treasury Department in 2024, with the US and French governments adding new elements to the attribution. Our investigation also found links between some of Doppelganger's activities and individuals associated with MGIMO (Moscow State Institute of International Relations).

ADVERSARIAL ADAPTATION IN RESPONSE TO ONGOING DETECTION

Our teams are engaged in daily efforts to find and block Doppelganger's attempts to come back to our apps. Here are some of our latest findings:

- **Shift in geographic targeting:** Starting in mid-November, the operators paused targeting of the US, Ukraine and Poland on our apps. It's still focused on Germany, France, and Israel with some isolated attempts to target people in other countries. Based on open source reporting, it appears that Doppelganger has not made this same shift on other platforms.

[1] Adversarial Threat Report, September 2022; Recapping Our 2022 Coordinated Inauthentic Behavior Enforcements, December 2022; Q4 2022 Report, February 2023; Q2 2023 Report, August 2023; Q3 2023 Report, November 2023; Q4 2023 Report, February 2024; Q1 2024 Report, May 2024, Q2 2024 Report, August 2024, Q3 2024 Report, December 2024.

- **Consistent low efficacy rate**: This operation continues to struggle to build authentic audiences on our apps, with the vast majority of their attempts at acquiring fake accounts or compromised Pages and running ads getting quickly detected and blocked, typically before anyone sees them.
- **Still no 'doppel' in Doppelganger:** As we noted in our previous report, Doppelganger's operators ceased to share links to external websites at the core of this operation's activity. We assess that this change is in response to our consistent blocking of their domains. We do, however, continue to see that Doppelganger maintains these off-platform websites that spoof large news organizations, which suggests that the operators are attempting to seed these links and amplify these deceptive sites elsewhere on the internet.
- **Memes to nowhere:** Likely to avoid automated detection of links and keywords, Doppelganger has reduced itself to posting minimal text overlaid on images that lead nowhere (i.e. no links) and build no audience. It continues to use compromised Pages, unrelated to politics or even countries typically targeted by this campaign.

Images: examples of Doppelganger attempted ads by a Vietnam-based page and a page from the Philippines. They were blocked and never ran. **On the left:** Auto-translated text–"He will defend the interests of the old gentlemen even to Germany's disadvantage". **On the right:** Auto-translated text – "America can rejoice - France is already completely dependent on it and Brussels".

- **Narrative shifts:** Although the war in Ukraine continues to feature in Doppelganger's content, since our last report in December, the operators appear to have shifted to painting the US as an unreliable partner to France, Germany and Israel claiming that they should break free from US influence. While operators avoid directly naming politicians or political parties (likely to try to avoid detection), some of their posts use images resembling the French President Macron and German politician Friedrich Merz claiming they are closely aligned with the US and therefore willing to sacrifice the interests of their own countries.
- **Looking forward:** We expect that influence campaigns like Doppelganger – no matter how ineffective – will likely continue trying to adapt to our detection because they are run by for-hire operators paid to keep at it by their clients. However, it appears that this campaign views Meta as a less useful platform and, as open source reporting suggests, it continues to run at higher volumes elsewhere.

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.

BENIN-BASED CIB NETWORK

Tactic	Threat indicator
Acquiring Assets	
Acquiring Facebook accounts	16 accounts
Acquiring Facebook Pages	6 Pages
Acquiring domains to support influence operations	newwayforward[.]us
Acquiring other online accounts	x[.]com/newwayforwardus
Disguising Assets	
Adopting visual disguise	This campaign used profile photos likely generated using artificial intelligence
Impersonating real person	In the US, they ran an off-platform website – which mimicked the Harris campaign site. While the website appeared to look like the real

	campaign site, its *Issues* page contained fictitious claims about the campaign's positions including on the aid to Ukraine.
Evading Detection	
Obfuscating infrastructure	The operators used proxy IP infrastructure to conceal their origin and appear as if they were in France
Targeted Engagement	
Running Ads	About $1,300 in spending for ads, paid for mostly in US and Canadian dollars.
Engaging with users outside the operation	About 18,000 accounts followed one or more of these Pages
Engaging with specific audience	This effort targeted primarily France with posts in French about news and current events
Posting about individuals or institutions	The campaign posted criticism of President Macron, and NATO
	The campaign posted supportive commentary about Marine Le Pen and her party

GHANA-BASED CIB NETWORK

Tactic	Threat indicator
Acquiring Assets	
Acquiring Facebook accounts	42 accounts
Acquiring Facebook Pages	1 pages
Acquiring Instagram accounts	33 accounts
Acquiring domains to support influence operations	empoweringghana[.]com
Acquiring other online accounts	x[.]com/empoweringghana
	x[.]com/YamoahFestus

	youtube[.]com/@EmpoweringGhana
	tiktok.com/@empoweringghana
Disguising Assets	
Adopting visual disguise	Using profile photos likely generated using artificial intelligence such as Generative Adversarial Networks (GAN)
Posing as non-existent person	Posing as fictitious journalists and activists across many apps and on the EG website.
Posing as non-existent institution	This operation centered around a fictitious youth movement Empowering Ghana (EG) which had its own website and presence on multiple internet platforms.
Indiscriminate Engagement	
Amplifying with fake accounts on Facebook, Instagram, X/Twitter	The operators used fake accounts to comment on posts by this fictitious movement, likely to make it appear to have local support
Targeted Engagement	
Running Ads	About $10,200 in spending for ads, paid for mostly in US dollars.
Engaging with users outside the operation	About 38,000 accounts followed one or more of these Pages
	About 880,000 accounts followed one or more of these Instagram accounts. The vast majority of Instagram followers were outside of Ghana, suggesting the use of fake engagement tactics to make this operation appear far more successful than it was
Engaging with specific audience	The people behind this activity posted about politics in Ghana, primarily in English
Posting about individuals or institutions	Posting supportive commentary about the former Vice President Bawumia who lost in the latest Presidential election.

CHINA-BASED CIB NETWORK

Tactic	Threat indicator
Acquiring assets	
Acquiring Facebook accounts	18 accounts
Acquiring Facebook Pages	2 Pages
Acquiring Facebook Groups	4 Groups
Acquiring Instagram accounts	5 accounts
Acquiring other online accounts	x[.]com/pemadol99851
Creating online petitions	change[.]org/p/oppose-the-militarization-of-the-siang-district-need-dialogue-not-guns
	change[.]org/p/support-the-formation-of-a-new-tibetan-government-in-exile
Acquiring other online accounts	puranchettri910[.]blogspot.com
	thlhasa[.]blogspot.com
Disguising Assets	
Posing as fictional journalist	The operation created a fictitious persona posing as a journalist in the Arunachal Pradesh region of India
Posing as fictional person in target region	Most of the accounts posed as Tibetan expats, showed little complexity and were used primarily to reshare particular content from real people
Evading Detection	

Obfuscating infrastructure	They used proxy IPs to conceal their origin and appear to be coming from India, Bhutan or Nepal
Indiscriminate Engagement	
Amplifying with likely fake accounts on Facebook	The individuals behind this activity used fake accounts to manage Pages, post and amplify other people's content.
Targeted Engagement	
Engaging with users outside the operation	About 2,400 accounts followed one or more of these Pages
	About 120 accounts joined one or more of these Groups
	About 100 accounts followed one or more of these Instagram accounts.
Engaging with specific audience	The network posted primarily in English and Tibetan about news related to Tibet and its politics
Directing audience to website	This campaign frequently amplified anti-Dalai Lama content posted by authentic voices including sharing links to websites like Storify News, Dakini Translations and Publications, and a Change dot org petition
Posting about individuals or institutions	The network posted criticism of exiled Tibetan leader the Dalai Lama, conspiracies about his travel and health, and claims that the United States is using him as a lever against China
	The individuals behind this activity posted supportive commentary about Ogyen Trinley Dorje, a self-exiled Tibetan buddhist leader, and the need to normalize relations between Tibet and China