NOVEMBER 2023

THIRD QUARTER

# Adversarial Threat Report

Ben Nimmo, Global Threat Intelligence Lead

Nathaniel Gleicher, Head of Security Policy

Margarita Franklin, Public Affairs Director, Security

Lindsay Hundley, Security Policy Manager

Mike Torrey, Security Engineer

Meta

# TABLE OF CONTENTS

## PURPOSE OF THIS REPORT

Our public threat reporting began over six years ago when we first shared our findings about coordinated inauthentic behavior (CIB) by a Russian covert influence operation. Since then, we have expanded our ability 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 regular threat reports to include other threats and our detailed insights — all in one place, 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 elsewhere on the internet (see Appendix).

We expect the make-up of these reports to continue to evolve in response to the changes we see in the threat environment and as we expand to cover new areas of our Trust & Safety work. This report is not meant to reflect the entirety of our security enforcements, but to share notable trends and investigations to help inform our 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 (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 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 *Section 4* for specific examples of our work to counter recidivism attempts.

## SUMMARY OF OUR FINDINGS

In our Q3 Adversarial Threat Report, we're sharing findings about three separate covert influence operations that violated our policy against CIB. Two of them originated in China, and one – in Russia. We are also including our insights into the global threat landscape ahead of next year with its many elections around the world. This section covers the latest research into deceptive activities originating in Russia, Iran and China – the most prolific geographic sources of foreign influence operations to date, in addition to trends we see in the information environment, including challenges posed by generative Artificial Intelligence (AI) that we're working to tackle alongside governments, researchers, and our industry peers.

**New CIB networks disrupted in Q3'2023:**

**1. China:** We removed 13 accounts and seven Groups in China that targeted primarily India and the Tibet region and, to a lesser extent, the United States. This small network operated fictitious personas on Facebook and X (formerly Twitter) posing as journalists, lawyers and human-rights activists. We found this activity as part of our internal investigation into suspected coordinated inauthentic behavior in the region.

**2. China:** We removed 4,789 Facebook accounts in China that targeted the United States and posed as Americans across different platforms to post about US politics and US-China relations. We removed this network before it was able to gain engagement from authentic communities on our apps. We found this activity as part of our internal investigation into suspected coordinated inauthentic behavior in the region.

**3. Russia:** We removed six Facebook accounts, one Page, and three Instagram accounts in Russia that targeted global English-speaking audiences. The network posted primarily in English about Russia's invasion of Ukraine and ran fictitious "media" brands. A number of Russian embassies and diplomatic missions promoted these branded Telegram accounts on Facebook, X (formerly Twitter) and YouTube. After we removed this network, it appears to have shifted its activity to other apps entirely, including creating another media brand in recent weeks. We found this activity as a result of our internal investigation into suspected coordinated inauthentic behavior in the region.

# 01

## China

**We removed 13 accounts and seven Groups for violating our policy against coordinated inauthentic behavior. This network originated in China and targeted primarily India and the Tibet region and, to a lesser extent, the United States.**

The people behind this network operated two distinct clusters of fictitious personas on Facebook and X (formerly Twitter), each targeting a particular region: Tibet and the Arunachal Pradesh region of India. They posed as journalists, lawyers and human-rights activists. Some of these personas used the same name and profile picture on Facebook and X, and posted the same content on each platform. Likely in an attempt to appear more authentic, different personas commented on and shared each other's posts. We removed this network before it was able to gain engagement from authentic communities on our apps.

The network posted mainly in English, and to a lesser extent in Hindi and Chinese, about regional news, culture, sports and travel in Tibet and Arunachal Pradesh. Notably, the Tibet-focused accounts posed as pro-independence activists who also accused exiled Tibetan leader the Dalai Lama and his followers of corruption and pedophilia. The  Arunachal Pradesh-focused accounts posted positive commentary about  the Indian army, Indian athletes and Indian scientific achievements, and accused the Indian government of corruption and supporting ethnic violence in the Indian state of Manipur. A handful of accounts posed as Americans and shared links to articles from mainstream US media like HuffPost, Breitbart, the Wall Street Journal, and Fox News.

We found this activity as part of our internal investigation into suspected coordinated inauthentic behavior in the region.

- *Presence on Facebook and Instagram:* 13 Facebook accounts and seven Groups
- *Followers:* About 1,400 accounts joined one of these Groups.

# 02

## China

**We removed 4,789 Facebook accounts for violating our policy against coordinated inauthentic behavior. This network originated in China and targeted the United States.**

The individuals behind this activity used basic fake accounts with profile pictures and names copied from elsewhere on the internet to post and befriend people from around the world. Only a small portion of such friends were based in the United States. They posed as Americans to post the same content across different platforms. Some of these accounts used the same name and profile picture on Facebook and X (formerly Twitter). We removed this network before it was able to gain engagement from authentic communities on our apps.

The people behind this activity posted in English about US politics and US-China relations. The same accounts would criticize both sides of the US political spectrum by using what appears to be copy-pasted partisan content from people on X. Notably, some posts included X-specific language, such as “RT” (i.e. retweet) or “@[particular X handles]”, suggesting that this operation had copied and pasted content from X to Facebook without editing it. In some instances, they retweeted posts by X’s owner. They also posted links to news articles from mainstream US media and reshared Facebook posts by real people, likely in an attempt to appear more authentic. Some of the reshared content was political, while other covered topics like gaming, history, fashion models, and pets.

Unusually, in mid-2023 a small portion of this network’s accounts changed names and profile pictures from posing as Americans to posing as being based in India when they suddenly began liking and commenting on posts by the other China-origin network focused on India and Tibet described earlier in this report.

We found this activity as part of our internal investigation into suspected coordinated inauthentic behavior in the region.

- *Presence on Facebook:* 4,789 Facebook accounts.

# 03

## Russia

**We removed six Facebook accounts, one Page, and three accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in Russia and targeted global English-speaking audiences. Our investigation found links to employees of RT, a Russian state-controlled media entity.**

After we took strong enforcement steps against Russian state-controlled media at the start of the Russian war against Ukraine, including demoting their posts and providing labels to users so they know the source of information globally, the individuals behind this latest CIB activity attempted to create two seemingly independent, grassroots media projects across multiple internet platforms. It included  Telegram, X (formerly Twitter), Facebook, TikTok, and YouTube.

On our platform, we observed two phases of this activity. First, they created two separate Pages posing as independent news entities – they were quickly disabled by our automated systems aimed at detecting fake accounts. Next, the individuals behind these Pages attempted to recreate Pages for the same brands using other fake and duplicate accounts. Overall, likely in an attempt to build an audience, the network made heavy use of generic hashtags such as #news and #world, with up to a dozen per post. We took down this latest cluster of activity before it was able to gain engagement from authentic communities.

The network posted primarily in English about Russia’s invasion of Ukraine, accusing Ukraine of war crimes and Western countries of “russophobia.” These “media” brands also posted critical comments about transgender rights and human rights in Western countries, especially the United States and France, and criticized US President Joe Biden and French President Emmanuel Macron. They also praised Russia’s activities in West Africa while criticizing French activity there. A number of Russian embassies and diplomatic missions promoted these branded Telegram accounts on Facebook, X (formerly Twitter) and YouTube. After we removed this network, it appears to have shifted its activity to other apps entirely, including creating another media brand in recent weeks.

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

- *Presence on Facebook and Instagram:* Six Facebook accounts, one Page, and three Instagram accounts
- *Followers:* About 1,000 accounts followed one or more of these Pages and about 1,000 accounts followed one or more of these Instagram accounts.

# 04

# Threat landscape ahead of 2024

As we close out our threat reporting this year,[1] we've collated some of our key insights into the global threat environment and trends we anticipate facing our society and industry as we go into 2024 with its many elections around the world, including in the United States. This section includes: the latest research into deceptive activities originating in Russia, Iran and China – the most prolific geographic sources of foreign interference campaigns to date, and trends we anticipate in the information environment next year, including the challenges posed by generative Artificial Intelligence (AI), that we're working to tackle alongside our industry peers, governments and researchers.

## 4.1. Top foreign interference sources

With the latest takedowns included in this report, China is now the third most common geographic source of foreign CIB campaigns we've disrupted under our CIB policy, after Russia and Iran.

While these known campaigns have been disrupted by individual platforms, many of them remain active elsewhere on the internet and focus on politics in multiple parts of the world. Overall, these networks have continued to struggle to build audiences and shift to smaller platforms, but they're a warning – foreign threat actors are attempting to reach audiences ahead of next year's various elections, including in the US and Europe, and we need to remain alert to their evolving tactics and targeting across the internet.

Based on our ongoing work to detect and remove recidivist attempts by these networks and threat research into new inauthentic behavior, here are a few updates on the threat landscape related to Russia, Iran and China.

[1] Our Q4'2023 report will publish in Q1 of 2024

## Russia

Russia remains the most prolific geographic source of CIB networks in the world. Yet, for nearly two years now – since its full-scale invasion of Ukraine in February 2022 – Russia-based covert influence operations have focused primarily on the war and attempts to undermine international support for Ukraine. This applies to both CIB networks we took down on our apps, and their activity elsewhere on the internet which continues to this day.

We've recently found a new cluster of websites (outside of our platforms) linked to an extremely persistent operation known as "Doppelganger." These sites focus directly on US and European politics. The US-focused sites have names like Election Watch, Lies of Wall Street, Spicy Conspiracy, Truthgate, and 50 States of Lie. Their latest web content appears to have been copy-pasted from mainstream US news outlets and altered to question US democracy and promote conspiratorial themes. Soon after the Hamas terrorist attack in Israel, we saw these websites begin posting about the crisis in the Middle East as a proof of American decline; and at least one website claimed Ukraine supplied Hamas with weapons. Other websites in the same cluster focus on politics, migration and border security in France and Germany, with names including Le Belligérant, Les Frontières, Wanderfalke and Der Leitstern. This activity suggests an expansion of Doppelganger's focus from focusing primarily on Ukraine and foreign policy issues to also posting about domestic politics in the US and EU.

As before, we haven't seen these websites get much amplification by authentic audiences on our platform. We've updated our full list of threat indicators linked to Doppelganger with these and other latest domains, in addition to sharing them on GitHub in a machine-readable format.

## Iran

Historically, Iran has been the second most frequent country of origin of CIB networks we've taken down. While we have seen fewer novel Iranian-origin operations recently, we continued to detect and enforce against attempts by previous CIB networks to re-establish operations. Our work against Iranian foreign interference campaigns since 2017 has also enabled us to keep refining our understanding of their tactics and attribution.

For example, as part of our continuous enforcement against attempts to come back by networks we previously removed, we recently took down a set of accounts and Pages that targeted audiences in Afghanistan and were linked to a CIB network we disabled in October 2020. With that, we've now been able to link both the latest activity and originally unattributed operation to the Iranian state broadcaster, IRIB.

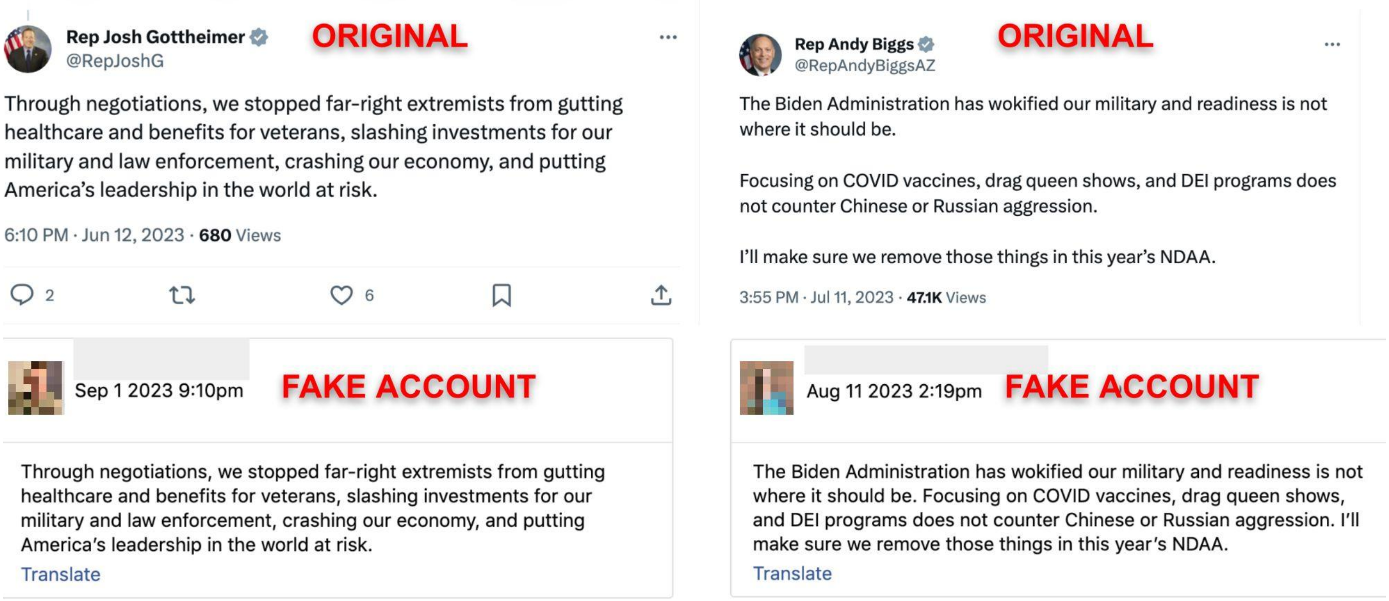
Also last quarter, we disabled a handful of unattributed Instagram accounts from Iran – under our Inauthentic Behavior policy – that posed as a conservative news outlet in the United States. This brand appears to be active on Telegram, YouTube, Gab, Gettr, and Truth Social. This cross-platform activity includes copy-pasting of content from authentic conservative voices on both sides of the Atlantic. Unusually for the operations we have seen from Iran, this one occasionally posts criticism of Iran and its regional allies on other platforms, amidst far more numerous criticisms of the US government.

## China

We've taken down five CIB networks from China targeting foreign audiences this year - more than from any other country. Most of these campaigns began in or after mid-2021, and failed to build authentic audiences. For comparison, between 2017 and November 2020, we took down two CIB networks from China, and both mainly focused on the Asia-Pacific region. This represents the most notable change in the threat landscape, when compared with the 2020 election cycle.

The latest operations – regardless of who was behind them – typically posted content related to China's interests in different regions worldwide. For example, many of them praised China, some of them defended its record on human rights in Tibet and Xinjiang, others attacked critics of the Chinese government around the world, and posted about China's strategic rivalry with the US in Africa and Central Asia. One operation, which we exposed in September 2022, initially focused on US domestic politics, but then changed its fake personas to focus on Czechia at a time when that country was debating leaving the "16+1" diplomatic format with China.

Similarly, the larger of the two operations we included in this Q3 threat report focused on domestic politics in the United States. Its fake accounts on Facebook copy-pasted posts from American politicians on both sides of the aisle on X (formerly Twitter) - including former House Speaker Nancy Pelosi, Governors Gretchen Whitmer and Kristi Noem, the "war room" of Governor Ron DeSantis, Senators Mark Kelly and Marsha Blackburn, and Representatives Sylvia Garcia, Terri Sewell, Matt Gaetz and Jim Jordan. It's unclear whether this approach was designed to amplify partisan tensions, build audiences among these politicians' supporters, or to make the fake accounts sharing authentic content appear more genuine *(see examples of this activity below)*.



Rep Josh Gottheimer
@RepJoshG

ORIGINAL

Through negotiations, we stopped far-right extremists from gutting healthcare and benefits for veterans, slashing investments for our military and law enforcement, crashing our economy, and putting America's leadership in the world at risk.

6:10 PM · Jun 12, 2023 · **680** Views

[redacted]
Sep 1 2023 9:10pm

FAKE ACCOUNT

Through negotiations, we stopped far-right extremists from gutting healthcare and benefits for veterans, slashing investments for our military and law enforcement, crashing our economy, and putting America's leadership in the world at risk.

Rep Andy Biggs
@RepAndyBiggsAZ

ORIGINAL

The Biden Administration has wokified our military and readiness is not where it should be.

Focusing on COVID vaccines, drag queen shows, and DEI programs does not counter Chinese or Russian aggression.

I'll make sure we remove those things in this year's NDAA.

3:55 PM · Jul 11, 2023 · **47.1K** Views

[redacted]
Aug 11 2023 2:19pm

FAKE ACCOUNT

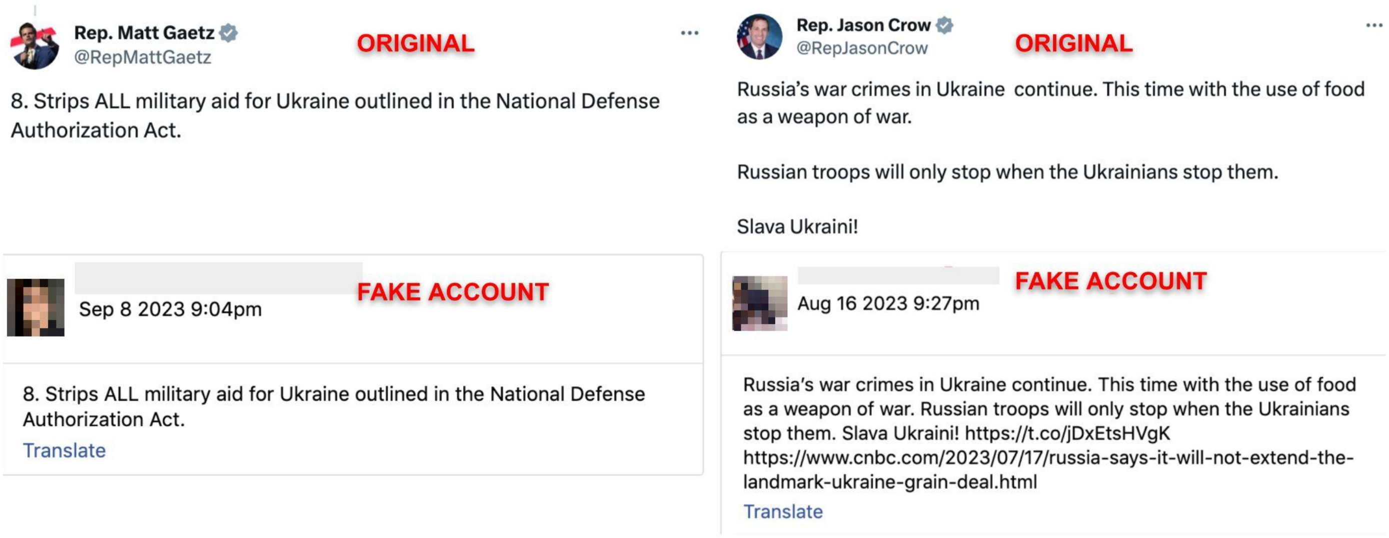
The Biden Administration has wokified our military and readiness is not where it should be. Focusing on COVID vaccines, drag queen shows, and DEI programs does not counter Chinese or Russian aggression. I'll make sure we remove those things in this year's NDAA.

**Images**

Top left and right, tweets by Reps Josh Gottheimer (D) and Andy Biggs (R).

Bottom left and right, Facebook posts by the China-origin network, copying/pasting the tweets by these elected representatives.

---



Rep. Matt Gaetz
@RepMattGaetz

ORIGINAL

8. Strips ALL military aid for Ukraine outlined in the National Defense Authorization Act.

[redacted]
Sep 8 2023 9:04pm

FAKE ACCOUNT

8. Strips ALL military aid for Ukraine outlined in the National Defense Authorization Act.

Rep. Jason Crow
@RepJasonCrow

ORIGINAL

Russia's war crimes in Ukraine  continue. This time with the use of food as a weapon of war.

Russian troops will only stop when the Ukrainians stop them.

Slava Ukraini!

[redacted]
Aug 16 2023 9:27pm

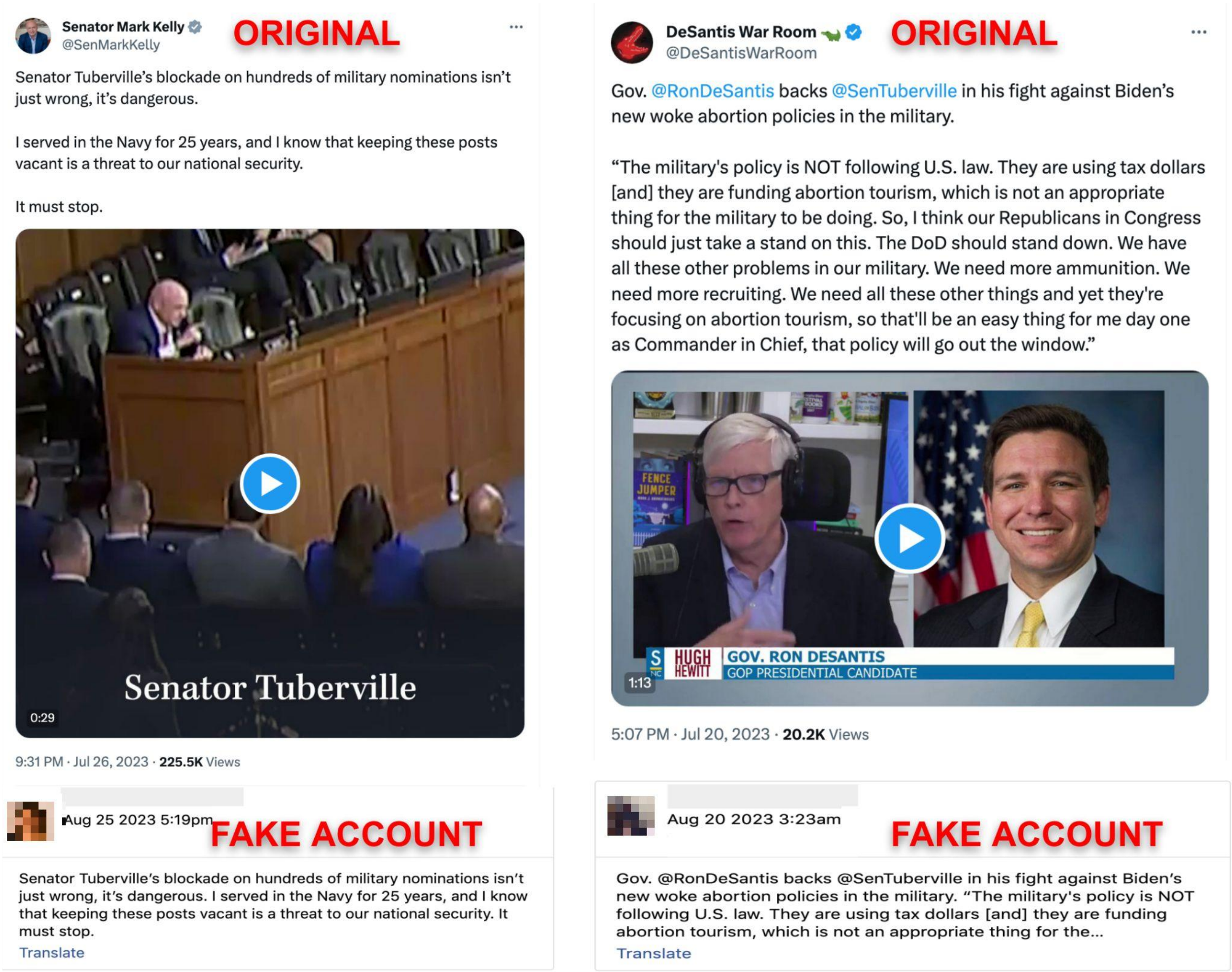
FAKE ACCOUNT

Russia's war crimes in Ukraine continue. This time with the use of food as a weapon of war. Russian troops will only stop when the Ukrainians stop them. Slava Ukraini! https://t.co/jDxEtsHVgK https://www.cnbc.com/2023/07/17/russia-says-it-will-not-extend-the-landmark-ukraine-grain-deal.html

**Images**

Top left and right, tweets by Reps Matt Gaetz (R) and Jason Crow (D).

Bottom left and right, Facebook posts by the China-origin network, copying/pasting the tweets by these elected representatives.



Senator Mark Kelly
@SenMarkKelly

Senator Tuberville's blockade on hundreds of military nominations isn't just wrong, it's dangerous.

I served in the Navy for 25 years, and I know that keeping these posts vacant is a threat to our national security.

It must stop.

9:31 PM · Jul 26, 2023 · **225.5K** Views

DeSantis War Room
@DeSantisWarRoom

Gov. @RonDeSantis backs @SenTuberville in his fight against Biden's new woke abortion policies in the military.

"The military's policy is NOT following U.S. law. They are using tax dollars [and] they are funding abortion tourism, which is not an appropriate thing for the military to be doing. So, I think our Republicans in Congress should just take a stand on this. The DoD should stand down. We have all these other problems in our military. We need more ammunition. We need more recruiting. We need all these other things and yet they're focusing on abortion tourism, so that'll be an easy thing for me day one as Commander in Chief, that policy will go out the window."

5:07 PM · Jul 20, 2023 · **20.2K** Views

[redacted]
Aug 25 2023 5:19pm

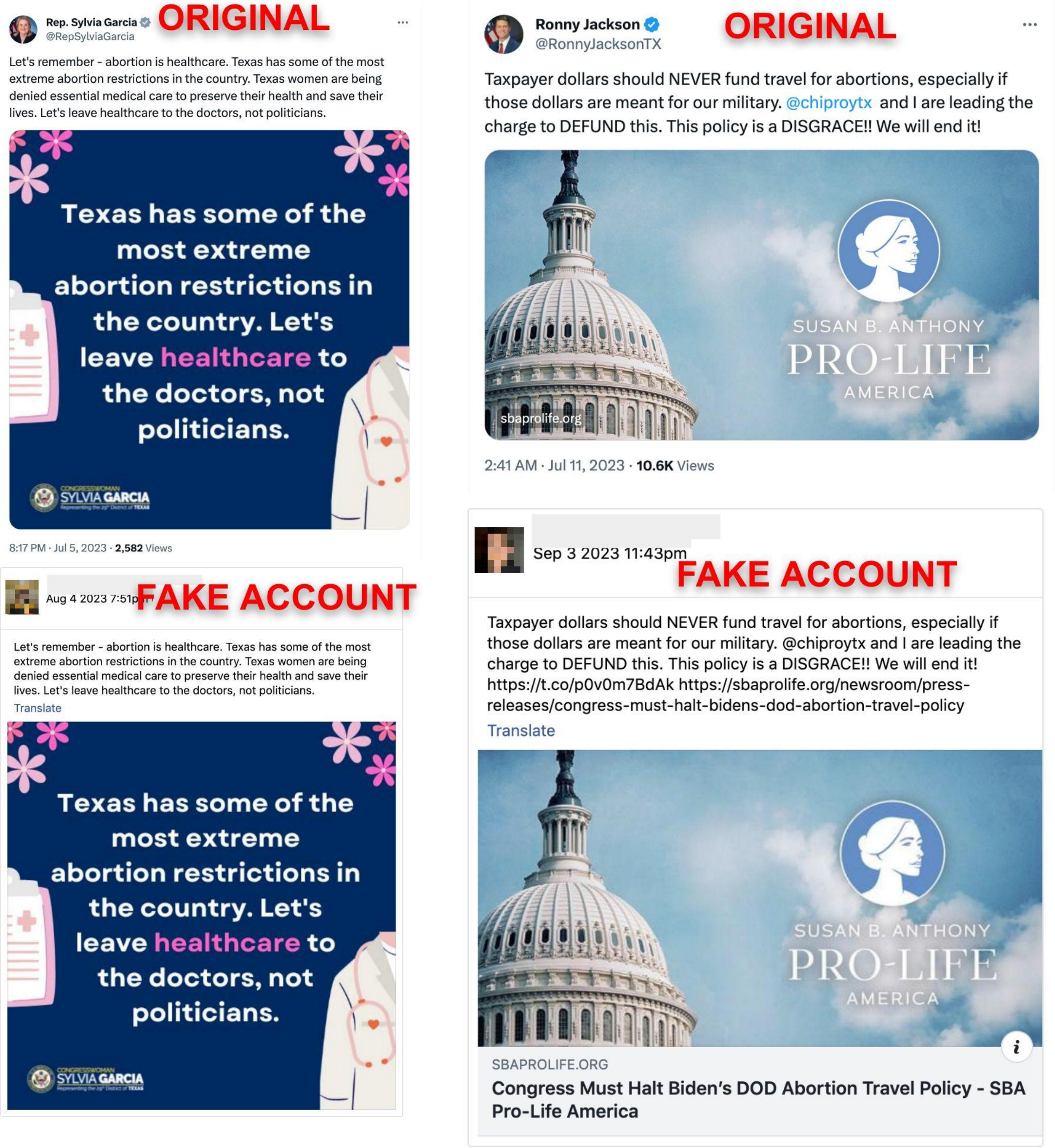
Senator Tuberville's blockade on hundreds of military nominations isn't just wrong, it's dangerous. I served in the Navy for 25 years, and I know that keeping these posts vacant is a threat to our national security. It must stop.
Translate

[redacted]
Aug 20 2023 3:23am

Gov. @RonDeSantis backs @SenTuberville in his fight against Biden's new woke abortion policies in the military. "The military's policy is NOT following U.S. law. They are using tax dollars [and] they are funding abortion tourism, which is not an appropriate thing for the...
Translate

**Images**

Top left and right, tweets by Senator Mark Kelly (D) and Senator Ron DeSantis' "war room" (R).  Bottom left and right, Facebook posts by the China-origin network, copying/pasting the tweets by these elected representatives.


ORIGINAL
ORIGINAL
FAKE ACCOUNT
FAKE ACCOUNT

Rep. Sylvia Garcia
@RepSylviaGarcia

Let's remember - abortion is healthcare. Texas has some of the most extreme abortion restrictions in the country. Texas women are being denied essential medical care to preserve their health and save their lives. Let's leave healthcare to the doctors, not politicians.

Texas has some of the most extreme abortion restrictions in the country. Let's leave healthcare to the doctors, not politicians.
CONGRESSWOMAN SYLVIA GARCIA

8:17 PM · Jul 5, 2023 · **2,582** Views

Ronny Jackson
@RonnyJacksonTX

Taxpayer dollars should NEVER fund travel for abortions, especially if those dollars are meant for our military. @chiproytx and I are leading the charge to DEFUND this. This policy is a DISGRACE!! We will end it!

2:41 AM · Jul 11, 2023 · **10.6K** Views

[redacted]
Aug 4 2023 7:51pm

Let's remember - abortion is healthcare. Texas has some of the most extreme abortion restrictions in the country. Texas women are being denied essential medical care to preserve their health and save their lives. Let's leave healthcare to the doctors, not politicians.
Translate

Texas has some of the most extreme abortion restrictions in the country. Let's leave healthcare to the doctors, not politicians.
CONGRESSWOMAN SYLVIA GARCIA

[redacted]
Sep 3 2023 11:43pm

Taxpayer dollars should NEVER fund travel for abortions, especially if those dollars are meant for our military. @chiproytx and I are leading the charge to DEFUND this. This policy is a DISGRACE!! We will end it! https://t.co/p0v0m7BdAk https://sbaprolife.org/newsroom/press-releases/congress-must-halt-bidens-dod-abortion-travel-policy
Translate

SBAPROLIFE.ORG
**Congress Must Halt Biden's DOD Abortion Travel Policy - SBA Pro-Life America**

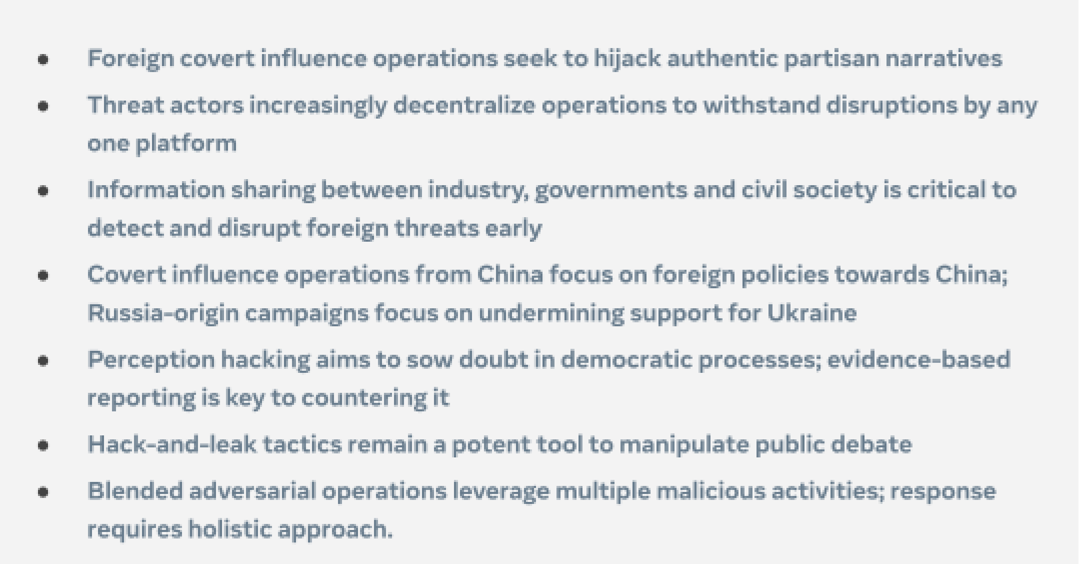
**Image**

Top left and right, tweets by Reps Sylvia Garcia (D) and Ronny Jackson (R).

Bottom left and right, Facebook posts by the China-origin network, copying the tweets by these elected representatives.

## 4.2. Information environment ahead of 2024

As we head into the new year, here are some key threat insights and trends we wanted to highlight for the security community to help inform our collective defenses in the evolving information environment globally:



- Foreign covert influence operations seek to hijack authentic partisan narratives
- Threat actors increasingly decentralize operations to withstand disruptions by any one platform
- Information sharing between industry, governments and civil society is critical to detect and disrupt foreign threats early
- Covert influence operations from China focus on foreign policies towards China; Russia-origin campaigns focus on undermining support for Ukraine
- Perception hacking aims to sow doubt in democratic processes; evidence-based reporting is key to countering it
- Hack-and-leak tactics remain a potent tool to manipulate public debate
- Blended adversarial operations leverage multiple malicious activities; response requires holistic approach.

### Hijacking authentic partisan narratives

As our report shows, influence operations try to leverage authentic partisan debate as part of their deceptive campaigns. As we shared in Section 4.1, rather than creating original content, the recent activity from both China and Iran copied partisan posts from real people, including influential political figures. For example, they pasted tweets verbatim from X (formerly Twitter) onto Facebook or Telegram. This can be done to obfuscate the fact they are a direct 'copypasta' or to exacerbate already existing tensions in the target countries. It can also be an attempt to promote narratives that the operators support, or to build an initial audience to be targeted with other narratives later.

Influence operators are not the only malicious actors that we've seen using this tactic. With every major civic moment or crisis, we also expect and continuously enforce against financially-motivated spammers and scammers who latch onto trending topics. They may attempt to monetize partisan narratives by copying content from real news outlets and people and using it to drive traffic to off-platform websites filled with pay-per-click ads.

These examples of 'copypasta' tactics used by malicious campaigns also show why relying on content alone is not enough when determining whether an account is part of an influence operation or adversarial campaign. Mislabeling authentic political commentary as a ‘bot’ can not only quash real public discourse, but can lead to diminishing trust in democratic processes overall. And because we have already seen threat actors seek to hijack partisan narratives for their own ends, it is especially important to be deliberate when posting and engaging with political content across the internet and to check who is sharing it.

## Decentralizing to withstand disruptions

We’ve seen an increasing number of CIB networks widely spread their assets and infrastructure across many internet surfaces, rather than centralizing their activity and coordination in one place. Spamouflage, the China-origin operation that we and our industry peers have been tracking, is a good example. It was seen running on 50+ platforms, and it primarily seeded content on blogging platforms and forums like Medium, Reddit and Quora before sharing links to that content on ours.

This trend can be a function of larger platforms keeping up the pressure on threat actors, which pushes them to move to smaller services in the hope of facing less scrutiny. It may also be why many operations now run their own websites which allow some degree of resiliency against any one platform disabling activity on a particular app. We expect this trend to accelerate as more platforms monitor potentially violating activity around many elections in 2024. Relatedly, domain abuse is one area where existing mechanisms to redress abuse are not sufficient to have material impact at scale. We believe that, in addition to legal and enforcement steps taken by platforms like ours,  industry-wide action is needed to protect people against these tactics and raise our collective defenses and we shared our recommendations in our Q2 '2023  threat report.

This expansion of platform targeting by deceptive campaigns provides a valuable signal that the cross-industry threat disruption approach can be effective in making malicious activity harder to sustain for longer periods of time. It also increases the cost of running these operations for threat actors as they spread themselves thinner across the internet. However, this shift also demonstrates how critical it is to continue threat sharing across our industry and with the public so that all apps – big or small – can benefit from threat research by others in identifying potential adversarial threats.

As part of supporting this effort, we’ve included threat indicators for the latest CIB operations in the Appendix, to support the open-source community and enable further research. We’re also making these indicators available on Github in a machine-readable format.

### Information sharing between industry, governments and civil society

Sharing information between tech companies, governments and law enforcement has also proven critical to identifying and disrupting foreign interference early, ahead of elections. As an example, prior to the 2020 elections, we investigated and took down three covert influence operations from Russia, Mexico and Iran targeting the US, after receiving a tip from US law enforcement about off-platform activity by these threat actors.

This type of information sharing can be particularly critical in disrupting malicious foreign campaigns by sophisticated threat actors who coordinate their operations outside of our platforms. While we've continued to strengthen our internal capacity to detect and enforce against malicious activity since 2017, external insights from counterparts in government, as well as researchers and investigative journalists, can be particularly important in detecting and disrupting threat activity early in its planning taking place off-platform. While information exchange continues with experts across our industry and civil society, threat sharing by the federal government in the US related to foreign election interference has been paused since July.

We believe it's important that we continue to build on the progress the defender community has made since 2016, and make sure we work together to keep our defenses against foreign interference strong.

### Narrative focus from Russia and China

As we noted earlier in this report, recent influence operations from both China and Russia have focused on particular geopolitical themes. These narratives of interest are likely to draw further influence attempts from these sources if they come into play in the election debates in Europe and the United States.

Specifically, we anticipate that if relations with China become an election issue in a particular country, it is likely that we'll see China-based influence operations pivot to attempt to influence those debates. In addition, the more domestic debates in Europe and North America focus on support for Ukraine, the more likely that we should expect to see Russian attempts to interfere in those debates.

### Perception hacking

Just like in 2020, we expect IO actors to engage in what we call "perception hacking" – that is, rather than running actual on-platform campaigns or compromising election systems, they attempt to garner influence by fostering the perception that they are everywhere, playing on people's fear of widespread deception itself.

During previous US election cycles, we identified Russian and Iranian operations that claimed they were running campaigns that were big enough to sway election results, when the evidence showed that they were small and ineffective. IO-for-hire services also routinely exaggerate their effectiveness to market their services and attract new clients – for example, by purchasing fake engagement (Q2'2022 report, p.19) to make their content look more popular than it is or by touting capabilities that leverage the latest technology without evidence of its efficacy.

Perception hacking aims to sow doubt in democratic processes or in the very concept of "facts" without the threat actors actually having to impact the process itself. Similarly, accusations of foreign interference by authentic political groups leveled at people they disagree with, without any evidence to back up such claims, can have the same effect of sowing distrust in electoral outcomes and public institutions.

One defense against perception hacking is: fact-based, routine and predictable threat reporting. This is also a way for defenders to signal about the threats they are *not* seeing in a meaningful way. When claims emerge of influence operations, it's critical to weigh them against the evidence, including whether they reached any kind of authentic audience across the internet or broke through with traditional media.[2] Historically, while a few operations have built up sizable followings across many platforms, many more have failed to reach any kind of audience at all. Our work since 2017 has shown that the existence of CIB campaigns does not automatically mean they are successful.

### Hack and leak tactics

Early this year, we disrupted an Iranian CIB network that ran a series of fake "hacktivist" personas, and offered to publish allegedly hacked documents in countries including France. We also took down a for-hire network run from the US and Venezuela that targeted Honduras with a fake hacktivist persona called "HondurasLeaks."

Posing as "hacktivists" or civically engaged personas to spread hacked or fictitious leaks is a practice we've regularly observed in influence operations. For example, in 2019, the Russian operation "Secondary Infektion" distributed materials that were proven to have been hacked from a UK government minister shortly before the UK general election. In 2020, an Iranian operation posed as the "Proud Boys" group in the US and claimed to have hacked US election systems. Last year, a suspected Russian operation reportedly compromised Moldovan officials' Telegram accounts and released alleged evidence of electoral fraud from those officials' private

[2] The Breakout Scale is a tool designed for the open-source community to assess the impact of influence operations.

communications, while the government claimed the posts were manipulated and taken out of context.

We expect that this tactic will remain a potent tool to manipulate public debate – either through releasing hacked materials wholesale, or claiming to possess them to sow uncertainty and force people to prove a negative in the absence of evidence, or publishing distorted documents while claiming their authenticity. This can be particularly challenging to counter in the time-pressured context of election news reporting.

GenAI-created multimedia claiming to be hacked materials can further add to this challenge. While we haven't seen evidence of this technology being used by known covert influence operations to make hack-and-leak claims *(see GenAI in the Spotlight section below)*, we all need to remain vigilant to monitor how GenAI might enable this centuries-old tactic of forging evidence to advance one's strategic goals.

As we all prepare for 2024, it is especially important for political campaigns, candidates, public figures and media outlets to keep their cyber defenses up to date, as these all represent attractive potential targets for hackers. On our platforms, we will continue to remove content that shares or claims to share material obtained from a hacked source, except in limited cases of newsworthiness.

### Blended operations

In addition to covert influence operations, we've seen threat actors engage in what we call "blended" operations that involve more than one type of adversarial activity. For example, a network from Bolivia that we exposed earlier this year used fake accounts to create fictitious media brands and share content supportive of the MAS party while also attempting to abuse our reporting systems. They did so by filing a large number of false reports against people critical of the party, including news organizations and members of the opposition, with the apparent goal of getting them taken down.

Similarly, the operation known as  Ghostwriter, and an unrelated Azeri network we removed last year, both compromised their targets' social-media accounts and websites and used them to post false stories, combining hacking and influence operations. We've also seen influence operations leverage fake followers likely acquired from account farms in various countries, including Vietnam and Bangladesh, to appear more popular than they were by adopting some spam-like techniques.

Tackling these cross-internet threats requires a broader, holistic approach. Traditionally, the defender community has tended to treat each of these threats - influence operations, espionage, spam and others - in silos. But by comparing them, we can identify more ways to disrupt and counter them earlier in their lifecycle, based on common behavioral patterns. To aid in this effort and share our internal learnings, we published an online operations killchain to provide a framework for comparing and mapping these different types of operation. The framework helps identify common tactics across different types of operation, which in turn enables defenders to invest in defenses that have the biggest potential impact across many different threats.

## Generative AI in the spotlight

In addition to the threat landscape we described above, we wanted to dive deeper into the challenges and opportunities associated with Generative AI (GenAI) and how we can strengthen our collective defenses against malicious groups leveraging these new technologies.

### State of play

Before we go into the GenAI-related risks and opportunities we see ahead of next year, here is how we've seen threat actors leverage AI-generated content to date:

- 📷**Images:** In 2019, a network we took down in Vietnam and the US became the *first known* CIB operation to make use of profile pictures created using techniques like Generative Adversarial Networks (GAN). In 2022 more than two-thirds of all the CIB networks worldwide that we took down featured accounts that likely had GAN-generated profile pictures, in an apparent attempt to build credibility and appear unique.
- 🎥**Video:** While it was not part of a known on-platform operation, in early 2022, we identified and removed a 'deepfake' video that appeared to show Ukraine's President Zelensky making a statement he never did. It appeared on a reportedly compromised website and then started showing across the internet. In another example, earlier this year, we took down a cluster of accounts linked to the China-based influence operation "Spamouflage" that was reported by researchers at Graphika to have used AI-generated newsreaders in their videos on social media platforms including Facebook, Twitter, and YouTube. These early attempts at using AI-generated videos were quickly identified and exposed. To date, we have not seen evidence of this tactic being widely and successfully used by CIB networks we disrupted, including sophisticated threat actors.
- 🔉 **Audio:** Recently, we detected and removed a cluster of commenting activity by Spamouflage targeting audiences in Canada. Researchers at ASPI described this operation's use of likely GenAI audio in a doctored YouTube video shared on other platforms, with "zero or minimal engagement with real users".

Aside from threat actors we've taken down for CIB, we've seen examples where AI-generated content was posted online by various individuals. Many of these uses are innovative, exciting, and positive. But inevitably, some of this experimentation pushes the boundaries of what's acceptable, raising important societal questions. For example, we've seen instances across the internet where people posted audio purporting to be genuine recordings of public figures which were exposed as, or suspected to be, created by AI. As an example, we've seen a case when a political party in Poland reportedly used AI-created audio in the course of an election campaign to make an argument against their opponents.

## Existing Trust & Safety measures

As the defender community continues to assess the risks associated with rapidly evolving new technologies like AI, many of the existing defenses across our industry already apply: the majority of current concerns about generative AI relate to problematic behavior or content that is already understood by our industry and society at large. Here is how we look at both:

### Behavior

On the security side, our enforcements against determined adversaries like covert influence operators focus on their adversarial behavior, not the content they post – whether it's created using AI or not. In fact, we've seen examples when the use of AI-generated images by CIB campaigns tipped off researchers, including Meta's, to expose networks of fake accounts behind them. Further, by the time influence operations may leverage AI to create and post content, they will already have left numerous adversarial behavioral signals, such as how they acquire, disguise and coordinate their fake accounts, all of which can aid threat research and disruption efforts.[3]

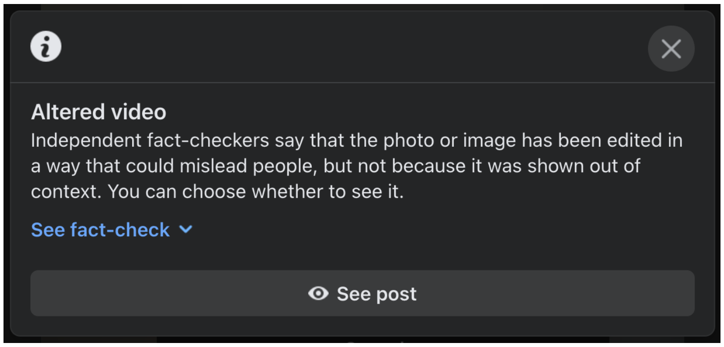
Overall, the use of manipulated and decontextualized media as part of malicious campaigns is the latest manifestation of a long-standing tactic deployed by influence operations (dating back to before the internet) that try to plant false content like forged documents or photoshopped images in an attempt to shape perception. For tech platforms, enforcing against this tactic means disrupting these operations according to existing policies against adversarial behaviors.

### Content

In addition to behavior-focused enforcements, our investments in AI over the last several years have allowed us to build technologies to proactively identify content that potentially violates our policies, prioritize the most critical content to be reviewed, and take action against violations of our

[3] The sequence of steps such operations may go through is described in the Online Operations Kill Chain, a framework that allows analysts to identify the earliest points at which an operation can be disrupted.

Community Standards. This applies to all content, which means we will remove any content that violates our policies including Instagram's Community Guidelines and our Ad Standards, regardless of whether it is created by AI or a person. We have also built a parallel content review system to flag posts that may be going viral—no matter what type of content it is—as an additional safety net in case that content violated our policies.

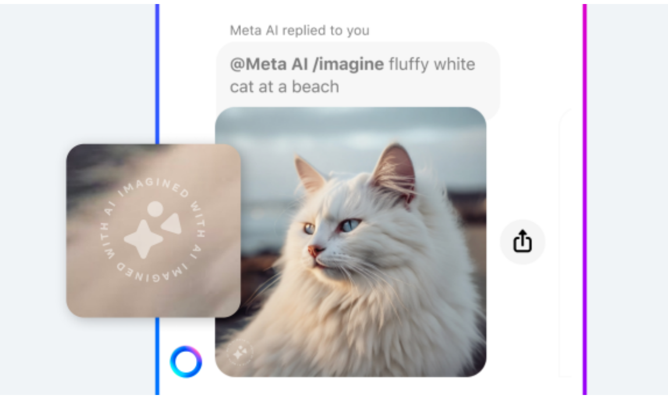


Altered video

Independent fact-checkers say that the photo or image has been edited in a way that could mislead people, but not because it was shown out of context. You can choose whether to see it.

Further, AI-generated content is eligible to be reviewed by nearly 100 independent fact-checking partners globally covering more than 60 languages. One of the rating options is *Altered*, which includes, "Faked, manipulated or transformed audio, video, or photos." As an example, if a misleading video is rated as *False* or *Altered* by our fact checking partners, it can be down-ranked in Feed so far fewer people see it. We also don't allow an ad to run if it's rated *False, Altered, Partly False*, or *Missing Context*.

In addition, images created or edited using Meta's own consumer generative AI features (e.g., /imagine) contain visible markers so people know the content was created by AI.



Meta AI replied to you

**@Meta AI /imagine** fluffy white cat at a beach

Starting in the new year, we will require advertisers to disclose whenever a social issue, electoral, or political ad contains a photorealistic image or video, or realistic sounding audio, that was digitally created or altered to:

- Depict a real person as saying or doing something they did not say or do; or
- Depict a realistic-looking person that does not exist or a realistic-looking event that did not happen, or alter footage of a real event that happened; or

- Depict a realistic event that allegedly occurred, but that is not a true image, video, or audio recording of the event.

## Cross-society challenges & opportunities

While the use of AI by known threat actors we've seen so far has been limited and not very effective, we want to remain vigilant and prepare to respond as their tactics evolve. Here are some key challenges we anticipate, and opportunities that would allow us all to raise our collective defenses as we head into 2024:

### 1. Scale of potentially misleading content

Generative AI can enable threat actors to create larger volumes of convincing content, including clickbait often used by financially-motivated actors like spammers or scammers and threat actors looking to engage with audiences for whom they don't have cultural expertise or language skills.

Combining this with a range of elections worldwide in 2024 means that the defender community across our society needs to prepare for a larger volume of synthetic content. This means that just as potentially violating content may scale, defenses must scale as well, in addition to continuing to enforce against adversarial behaviors that may or may not involve posting AI-generated content. At Meta, our integrity systems are already built to manage large volumes of content, and this work to continue scaling our defenses will become even more important next year.

### 2. Leveraging AI to scale trust & safety efforts

We believe that large language models (LLMs) and other AI tools provide significant opportunities for the defender community to counter online abuse at scale. AI is of course not new – Meta and other platforms have long integrated AI into integrity systems. For example, we developed AI technologies to match near-duplications of previously fact-checked content. We also built a tool called Few-Shot Learner that can adapt more easily to take action on new or evolving types of harmful content quickly, and it works across 100+ languages. Previously, we would have needed to gather thousands or even millions of examples to build a dataset large enough to train an AI model, and then do the fine tuning to make it work properly. Few-Shot Learner can train an AI model based on only a handful of examples.

Generative AI could also help us take down harmful content faster and more accurately than existing AI tools. We've started testing LLMs by training them on our Community Standards to help determine whether a piece of content violates our policies. These initial tests suggest the LLMs can perform better than existing machine learning models, or enhance ones like Few-Shot Learner.

We're optimistic that generative AI can help us enforce our policies and increase precision at global scale.

We're also using LLMs to remove content from review queues in certain circumstances when we're highly confident it does not violate our policies. This frees up capacity for our reviewers to focus on content that's more likely to violate. Finally, AI also powers our automated tools looking to spot fake accounts and spam-like activity when someone posts at great frequencies or rapidly friends thousands of users at once.

There is still much work to be done to keep evolving these systems and scaling our trust and safety work effectively, but LLMs have the potential to be game changing in this space - lowering costs, improving ability to detect and adapt to changes, and increasing efficiency.

### 3. Speed of content creation

The immediacy of the news environment, particularly in times of crisis or critical civic events like elections, already means that content can go viral quickly, especially if picked up by influential figures or media. GenAI can enable faster content creation, which threat actors can use to further increase this risk by quickly aiding misleading claims by AI-created imagery, audio or video in hopes to get them to break through on mainstream media, online and on the ground. Third-party fact-checkers and news organizations reporting from the frontlines of public debate are an important resource to help tackle these risks. We've seen them be effective in cases where content was created or altered with AI and other synthetic methods. For example, fact checkers identified and rated deceptive audio content in Slovakia during its latest election campaign, as well as an AI-generated video of President Biden.

Especially in the context of contentious elections, geopolitical crises, war or natural disasters, it's essential that we allow facts to be established, while reporting with appropriate caution and transparency about known limitations in the meantime.

It's also important to note that no single tool or entity on its own can be enough to protect the information environment. That's why information sharing between platforms, media organizations, and AI content creators can be critical in enabling timely analysis and fact-checking. While we realize that it might be challenging, cross-society collaboration can help inform our collective responses to manipulation given that AI-generated content doesn't stay within one platform and is likely to travel across the internet (see our recommendations for information sharing here).

### 4. Developing transparency and detection standards for AI content

While there aren't common standards for identifying and labeling AI-generated content across the industry, we believe there should be. While we are developing our own transparency measures according to industry best practices (e.g., visible markers on images, fact-checking labels, and our disclosure policy on political and social issue ads), we are also working with other companies through forums like the Partnership on AI (PAI) to help develop industry-wide approaches and advance ethical and responsible behavior by creators, social and traditional media, and AI companies.

In addition to PAI, we are working with governments around the world to lay the groundwork to ensure that AI innovations are safe, fair and trustworthy. For example, we signed onto the White House's voluntary commitments on AI in July 2023 along with several other AI companies. They were an important step in ensuring responsible guardrails are established as a model for other governments to follow. The White House's most recent executive order further builds on those commitments.

Similarly, the G7 Code of Conduct for AI is a significant step towards global standards that will help companies like ours as we develop and deploy AI responsibly. While there are still important details to resolve, we are encouraged by the momentum and look forward to working with governments around the world to support these crucial processes.

These efforts are even more critical because we know that adversarial actors like foreign interference operations rarely, if ever, target one single platform. This means that standard transparency measures might present a potent opportunity to help people know that the content – whatever AI tool helped create it – has been artificially generated. However, we know that threat actors will try to evolve their tactics to evade any new transparency standards or detection tools, which is why we continue to work with industry partners to develop more robust disclosure and provenance solutions. We'll also keep sharing our insights, including from AI research and threat ideation efforts, so we can all strengthen our collective defenses across society.

### 5. Building consensus on AI use in public discourse

Whereas foreign interference campaigns using AI-created content (or any other content for that matter) are seen as uncontroversially abusive and adversarial, authentic political groups and other domestic voices leveraging AI can quickly fall into a 'gray' area where people will disagree about what is permissible and what isn't. This may include political ads aided by AI like we've seen at the start of the 2024 US campaign season. While each platform continues to apply a range of mitigations to misleading content, there is more work to do across our society to arrive at a consensus of what constitutes acceptable use and what common transparency and disclosure frameworks should look like across the internet.

## Final takeaways

Although interest in AI, particularly generative AI, has soared this year, threat actors and others have been using AI to create content for several years. We haven't seen evidence of these efforts being particularly effective at this time: our security teams and our peers across industry and civil society have exposed them before they were able to build their audiences. This highlights two insights about how generative AI may impact efforts to counter threat actors online:

1. Because defenders leverage behavioral investigations to find CIB campaigns, content-based efforts to hide (e.g., through GAN-generated photos and other content) have not been particularly effective. AI-generated content is unlikely to change this dynamic.
2. For sophisticated threat actors, content generation hasn't been a primary challenge. They rather struggle with building and engaging authentic audiences they seek to influence. This is why we have focused on identifying adversarial behaviors and tactics used to drive engagement among real people. Disrupting these behaviors early helps to ensure that misleading AI content does not play a role in covert influence operations. Generative AI is also unlikely to change this dynamic.

While generative AI does pose challenges for defenders, at this time we have not seen evidence that it will upend our industry's efforts to counter covert influence operations – and it's simultaneously helping to detect and stop the spread of potentially harmful content. Our teams are monitoring these risks while in close contact with industry peers and other experts, and this assessment will continue to evolve. But it is encouraging that our defenses continue to endure, even as technology evolves.

# 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 at Meta 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. 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.

## 1. CHINA-BASED CIB NETWORK #1

| Tactic | Threat indicator |
|---|---|
| **Acquiring assets** | |
| *Acquiring Facebook accounts* | 13 accounts |
| *Acquiring Facebook Groups* | 7 Groups |
| *Acquiring Twitter / X accounts* | http://twitter[.]com/nickjonas154141 |
| | http://twitter[.]com/nehaji0521 |

| | |
|---|---|
| | http://twitter[.]com/grenabor |
| | http://twitter[.]com/huyou99443141 |
| | http://twitter[.]com/aadhyaprasd |
| | http://twitter[.]com/christinek79095 |
| | http://twitter[.]com/sharma_kvita |
| **Disguising assets** | |
| *Adopting visual disguise* | Copying profile picture |
| *Posing as non-existent person* | The operation's fake personas included posing as journalists in Arunachal Pradesh |
| | The operation's fake personas included posing as a non-existent advisor to Human Rights Watch |
| | The operation's fake personas included posing as Tibetan activists |
| *Backstopping* | Some of the operation’s fake accounts adopted the same fake persona on Facebook and X |
| **Evading detection** | |
| *Faking social interactions* | Fake accounts in the network replied to and commented on each other’s posts |
| **Indiscriminate engagement** | |
| *Amplifying on Twitter* | http://twitter[.]com/jerryro52857088 |
| | http://twitter[.]com/michell64142282 |

| | |
|---|---|
| | http://twitter[.]com/kalarbrian |
| | http://twitter[.]com/alexamorrow13 |
| | http://twitter[.]com/jordanl61185831 |
| | http://twitter[.]com/vladchered90302 |
| | http://twitter[.]com/shannon81025511 |
| | http://twitter[.]com/kellyro52068757 |
| **Targeted engagement** | |
| *Acquiring followers for Facebook Groups* | About 1,400 accounts joined one or more of these Groups |
| *Posting into specifically themed Groups* | The network posted into Groups focused on Arunachal Pradesh |
| *Posting negative content about named individuals* | The network accused the Dalai Lama of corruption and pedophilia, and accused the Indian government of corruption and supporting ethnic violence in the Indian state of Manipur. |

## 2. CHINA-BASED CIB NETWORK #2

| Tactic | Threat indicator |
|---|---|
| **Acquiring assets** | |
| *Acquiring Facebook accounts* | 4,789 accounts |
| *Acquiring Twitter / X accounts (this list represents a sample of the total activity we identified)* | https://twitter[.]com/BoltinMich2800 |
| | https://twitter[.]com/GuzowskiJo48073 |
| | https://twitter[.]com/JeroenWolf52208 |
| | https://twitter[.]com/NoelLam362767 |
| | https://twitter[.]com/BethKander76343 |
| | https://twitter[.]com/CranStuart908 |
| | https://twitter[.]com/longstaffe64991 |
| | https://twitter[.]com/Burtonj20 |
| | https://twitter[.]com/ThomasTa52187 |
| | https://twitter[.]com/KatieDewit13751 |
| | https://twitter[.]com/rothenburg39412 |

| | |
|---|---|
| | https://twitter[.]com/SaraFishma78511 |
| | https://twitter[.]com/SivaShanmu91620 |
| | https://twitter[.]com/DianKroes58999 |
| | https://twitter[.]com/RafaelGuer41210 |
| | https://twitter[.]com/VictoireCo24192 |
| | https://twitter[.]com/ZacharySte55735 |
| | https://twitter[.]com/EvanRosebe39823 |
| | https://twitter[.]com/JafarShain3481 |
| | https://twitter[.]com/MatroneMar36813 |
| | https://twitter[.]com/MichaelDon76093 |
| | https://twitter[.]com/nadine_dee68147 |
| | https://twitter[.]com/VorkLauren93030 |
| | https://twitter[.]com/LarryRo73154309 |
| | https://twitter[.]com/Jacquel81168990 |
| | https://twitter[.]com/laura_liis85097 |
| | https://twitter[.]com/MaxRolfe696958 |
| | https://twitter[.]com/SLutsching94346 |

| | |
|---|---|
| | https://twitter[.]com/CristinaIordan9 |
| | https://twitter[.]com/AlexLeaton52039 |
| | https://twitter[.]com/JennyBe08226528 |
| | https://twitter[.]com/SeanHickma64677 |
| | https://twitter[.]com/CarstenRus33525 |
| | https://twitter[.]com/PrinceNata62818 |
| | https://twitter[.]com/MFyldes88917 |
| | https://twitter[.]com/JosVisker64445 |
| | https://twitter[.]com/MarkDijksm70234 |
| | https://twitter[.]com/HannahStew72451 |
| | https://twitter[.]com/DiegoVilla63602 |
| | https://twitter[.]com/MirendaKri40322 |
| | https://twitter[.]com/MBrooks84412 |
| | https://twitter[.]com/hatfield53436 |
| | https://twitter[.]com/JoeHaddox386703 |
| | https://twitter[.]com/SilviaBlaz8131 |
| | https://twitter[.]com/XavierMuri51380 |

| | |
|---|---|
| | https://twitter[.]com/ManuelaIpp12770 |
| | https://twitter[.]com/FranciscoO62412 |
| | https://twitter[.]com/CandiceWat74232 |
| | https://twitter[.]com/frank_komp69658 |
| | https://twitter[.]com/RobBots123147 |
| | https://twitter[.]com/PeterM6783 |
| | https://twitter[.]com/DowleFranc45935 |
| | https://twitter[.]com/SkipperReb33451 |
| | https://twitter[.]com/soeter_maa44975 |
| | https://twitter[.]com/KennethPer30024 |
| | https://twitter[.]com/TurkinAndr8230 |
| | https://twitter[.]com/RachelMcCl80642 |
| | https://twitter[.]com/BavasChels6815 |
| | https://twitter[.]com/JanineSchu7537 |
| | https://twitter[.]com/CourtierDe63548 |
| | https://twitter[.]com/Christophe28453 |
| | https://twitter[.]com/RhiannonHi92045 |

| | |
|---|---|
| | https://twitter[.]com/EricaClark36754 |
| | https://twitter[.]com/AlexanderB53048 |
| | https://twitter[.]com/StijnenRic59220 |
| | https://twitter[.]com/ELifflande42231 |
| | https://twitter[.]com/ILoppach43606 |
| | https://twitter[.]com/FBesseghai11295 |
| | https://twitter[.]com/TrimarchiC79048 |
| | https://twitter[.]com/FrancoKong97181 |
| **Disguising assets** | |
| *Adopting visual disguise* | Copying profile pictures |
| *Backstopping* | Some of the operation’s accounts used the same names and profile pictures on Facebook and X |
| **Evading detection** | |
| *Copying authentic content* | The operation's fake accounts on Facebook copy-pasted the texts of tweets from real Americans, including politicians. |
| *Obfuscating infrastructure* | The operation used proxy IP addresses in the United States |
| **Indiscriminate engagement** | |
| Amplifying with fake accounts on social media | Amplifying with fake accounts on Facebook |

| | |
|---|---|
| | Amplifying with fake accounts on X/Twitter |
| **Enabling longevity** | |
| *Replacing infrastructure* | Acquiring new social media accounts to replace disabled ones |

## 3. RUSSIA-BASED CIB NETWORK

| Tactic | Threat indicator |
|---|---|
| **Acquiring assets** | |
| *Acquiring Facebook accounts* | 6 accounts |
| *Acquiring Facebook Pages* | 1 Page |
| *Acquiring Instagram accounts* | 3 Instagram accounts |
| *Acquiring Twitter / X accounts* | https://twitter[.]com/PeopleSayNews |
| | https://twitter[.]com/militarywave001 |
| *Acquiring TikTok accounts* | https://www.tiktok[.]com/@peoplesay05 |
| *Acquiring YouTube channels* | https://www.youtube[.]com/@PeopleSayofficial |
| | https://www.youtube[.]com/@MilitaryWaves |
| *Acquiring Telegram channels* | https://t[.]me/ps_peoplesay |
| | https://t[.]me/militarywave |
| | https://t[.]me/PeoplesPress |
| **Disguising assets** | |
| *Adopting visual disguise* | The operation created visual brands for its fictitious news outlets |

| | |
|---|---|
| *Creating fictitious news outlet* | People Say |
| | Military Wave |
| *Backstopping* | The operation maintained the same fictitious news outlets on Facebook, Instagram, X, YouTube, TikTok and Telegram |
| **Indiscriminate engagement** | |
| *Posting common or generic hashtags* | #ps |
| | #peoplesay |
| | #knowmore |
| | #news |
| **Targeted engagement** | |
| *Acquiring followers for Facebook Pages* | About 1,000 accounts followed one or more of these Pages |
| *Acquiring followers for Instagram accounts* | About 1,000 accounts followed one or more of these Instagram accounts |
| *Directing audience to off-platform content* | Directing audience towards Telegram channels |
| **Enabling longevity** | |
| *Changing platforms* | After we disabled it, the network focused its activity on other platforms, and appears to have given up on using our apps. |

| | |
|---|---|
| *Changing personas* | On October 13, the “People Say” Telegram channel announced that it was moving to a new brand, “The People’s Press”, in response to takedowns and blockages of its service. |

## 4. IRAN-BASED INAUTHENTIC BEHAVIOR CLUSTER

| Tactic | Threat indicator |
|---|---|
| **Acquiring assets** | |
| *Acquiring Twitter / X account* | https://twitter[.]com/SGTnewsNetwork |
| *Acquiring Telegram channel* | https://t[.]me/s/SGTnewsNetwork |
| *Acquiring YouTube channel* | https://www.youtube[.]com/c/SGTNewsNetwrok |
| *Acquiring accounts on online forums* | https://truthsocial[.]com/@SGTnewsNetwork |
| | https://gettr[.]com/user/sgtnewsnetwork |
| | https://gab[.]com/SGTnewsNetwork |
| | https://linktr[.]ee/SGTnews |
| **Disguising assets** | |
| *Posing as fictional military personnel* | The cluster posed as an American veteran |
| *Backstopping fictitious brand or organization across multiple websites* | The cluster adopted the same persona across multiple platforms |
| **Evading detection** | |
| *Copying authentic content* | Many of the operation's posts were copied, without attribution, from real people or institutions on social media. |

# Continuous enforcement: novel indicators from recidivist attempts

We monitor for, and enforce against, efforts to come back by networks we previously removed. Some of these networks may attempt to create new off-platform entities, such as websites or social media accounts, as part of their recidivist activity.

We're sharing some of these novel threat indicators related to recidivism attempts to enable further research by the open-source community into any related activity across platforms. 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.

## 5. IRAN-BASED RECIDIVIST CIB CLUSTER

| Tactic | Threat indicator |
|---|---|
| **Acquiring assets** | |
| *Acquiring domains* | https://afgreview[.]com/ |
| | https://afgreview[.]com/ |
| | http://www.tahlilroz[.]af/ |
| *Acquiring Twitter / X accounts* | www.Tahlilroz[.]com |
| | https://twitter[.]com/afg_review |
| *Acquiring Telegram channels* | https://twitter[.]com/Tahlilroz_af |

| | |
|---|---|
| | https://t[.]me/AfghanistanDevelopments |
| *Acquiring YouTube channel* | https://t[.]me/Tahlilroz_af |
| **Enabling longevity** | |
| *Replacing infrastructure* | Acquiring new social media accounts to replace disabled ones |

## 6. DOPPELGANGER: ITS LATEST BRANDS & SPOOFED DOMAINS

This section includes the latest domains spoofing news or government websites that we've identified as part of the Doppelganger campaign as of October 31, 2023, as well as the latest domains that attempt to establish their own brands.

In addition to these domains, we've identified hundreds more that the campaign uses to redirect people to its spoofed and branded domains. We've updated our full list of threat indicators linked to Doppelganger with these and other latest domains,  in addition to sharing them on GitHub in a machine-readable format.

### Domains spoofing news or government sites

| Domain | Registration date | Country likely targeted |
|---|---|---|
| fox-news[.]in | 10/18/2023 | USA |
| unian[.]pm | 10/13/2023 | Ukraine |
| jiraboom[.]pro (Hosted a spoof of Der Spiegel) | 9/23/2023 | Germany |
| rbk-sourse[.]digital | 9/16/2023 | Ukraine |
| lepoint[.]foo | 8/7/2023 | France |
| leparisien[.]pm | 8/3/2023 | France |
| polityka[.]pro | 8/29/2023 | Poland |
| pravda-ua[.]rest | 8/2/2023 | Ukraine |
| pravda-ua[.]space | 8/2/2023 | Ukraine |
| fox-news[.]top | 2/10/2022 | USA |

### Operation's websites and brands

| Domain | Registration date | Country likely targeted |
|---|---|---|
| interventionist[.]us | 8/22/2023 | USA |
| cropmarketchronicles[.]us | 7/5/2023 | USA |

| Domain | Registration date | Country likely targeted |
|---|---|---|
| grenzezank[.]com | 7/5/2023 | Germany |
| kaputteampel[.]com | 7/5/2023 | Germany |
| lexomnium[.]com | 7/5/2023 | France |
| truthgate[.]us | 7/5/2023 | USA |
| warfareinsider[.]us | 7/5/2023 | USA |
| rrn[.]media | 7/26/2023 | Global |
| omnam[.]life | 7/19/2023 | Israel |
| artichoc[.]io | 6/29/2023 | France |
| lebelligerant[.]com | 6/29/2023 | France |
| holylandherald[.]com | 6/19/2023 | Israel |
| acrosstheline[.]press | 2/27/2023 | USA |
| derleitstern[.]com | 2/27/2023 | Germany |
| derrattenfanger[.]net | 2/27/2023 | Germany |
| mypride[.]press | 2/27/2023 | USA |
| ukrlm[.]info | 2/27/2023 | Ukraine |
| allons-y[.]social | 2/24/2023 | France |
| candidat[.]news | 2/24/2023 | France |
| franceeteu[.]today | 2/24/2023 | France |
| laterrasse[.]online | 2/24/2023 | France |
| lavirgule[.]news | 2/24/2023 | France |
| lesfrontieres[.]media | 2/24/2023 | France |
| notrepays[.]today | 2/24/2023 | France |
| 50statesoflie[.]com | 2/23/2023 | USA |
| besuchszweck[.]org | 2/23/2023 | Germany |
| electionwatch[.]live | 2/23/2023 | USA |

| Domain | Registration date | Country likely targeted |
|---|---|---|
| honeymoney[.]info | 2/23/2023 | USA |
| liesofwallstreet[.]com | 2/23/2023 | USA |
| spicyconspiracy[.]info | 2/23/2023 | USA |
| uschina[.]press | 2/23/2023 | USA |
| wanderfalke[.]net | 2/23/2023 | Germany |