

DECEMBER 1, 2021

DETAILED REPORT

Adversarial Threat Report

By Nathaniel Gleicher, Head of Security Policy

Ben Nimmo, Global IO Threat Intelligence Lead

David Agranovich, Director, Threat Disruption

Mike Dvilyanski, Head of Cyber Espionage Investigations

SUMMARY

- We're sharing a detailed, end-of-year update on our progress against adversarial networks that we found and removed for different policy violations around the world: Coordinated Inauthentic Behavior (CIB), Brigading, and Mass Reporting. More details [here](#).
- We removed four CIB operations — from China, Palestine, Poland, and Belarus. In our November CIB report, we included a deep-dive research assessment into the China-based network and specific threat indicators to facilitate further research into this COVID-19-focused activity across the internet. More details [here](#).
- Last year, we launched a pilot research platform — built with CrowdTangle — where we're sharing data with independent OSINT researchers and scholars who study influence operations. We'll be expanding this archive to more researchers over the next several months. More details [here](#).
- As part of expanding our network disruption efforts to emerging threats, including from authentic groups, we took two separate enforcement actions under two new security policies.
- Under our Inauthentic Behavior policy against mass reporting, we removed a network in Vietnam for repeatedly and falsely reporting activists and government critics for policy violations to Facebook in an attempt to silence them. More details [here](#).
- Under our Brigading policy, we took down a network linked to the anti-vaccination movement called V_V which targeted medical professionals, journalists and elected officials in Italy and France to harass them across the internet, including on our platform. More details [here](#).

LAYERED DEFENSE APPROACH

The global threats that our teams tackle have significantly evolved since we first started sharing our findings about the influence operations we take down for Coordinated Inauthentic Behavior (CIB) in 2017. We see bad actors not only shift their tactics in response to our enforcement but they also, of course, don't strive to neatly fit our policies or only violate one at a time.

While our work began with tackling CIB networks of fake accounts meant to mislead people about who's behind them, we've also seen adversarial groups engage in harmful behaviors while using their authentic accounts. In fact, these networks often engage in multiple violating behaviors at once. For example, a coordinated network of largely authentic accounts might engage in mass harassment of activists through comments on their posts, while also maintaining dormant duplicate and fake accounts to persist on the platform in case their real accounts get disabled for repeated hate speech or other violations.

In this environment, we build our defenses with the expectation that adversarial groups will not stop, but rather adapt and try new tactics to persist. Our focus has been to study malicious behaviors and add new layers of defense to our arsenal to make sure we prevent and address potential gaps from multiple angles. Our goal over time is to make these behaviors more costly and difficult to hide, and less effective. It is a significant, ongoing effort that spans teams, departments and time zones across Meta.

Today's network disruption report *for the first time* brings together multiple takedowns for distinct violations of our security policies, including the first public takedowns under two new protocols launched in the last six months. The networks used different behaviors, but all have one thing in common — each actively coordinated to target people and abuse our systems. In this post, we will share our findings about six networks we recently removed around the world for Coordinated Inauthentic Behavior, Brigading, and Mass Reporting.

As we continue building our understanding of these emerging threats, we will keep sharing our findings with industry peers, independent researchers, law enforcement and policymakers — including on these new disruptions — so we can collectively improve our defenses. We welcome feedback from external experts as we refine our approaches.

SHARING ANALYSIS & DATA WITH RESEARCHERS

Many of our colleagues across the security teams at Meta come from the research community with decades of experience in studying and tackling influence operations, espionage, national security and other threats. Since 2018, we've been sharing information about over 150 networks we removed for CIB with independent researchers, because we know that no single organization can tackle these challenges alone. Thanks to this collaboration, we've greatly expanded our own understanding of internet-wide security risks and have seen about 100 investigations and assessment reports published for everyone to review and build on.

Over the past year and a half, we've been working closely with the CrowdTangle team at Meta to build a platform where researchers can access public data about these networks in one place to uncover insights by comparing tactics across threat actors globally and over time. In late 2020, we launched a pilot CIB archive where we've since shared nearly 100 of the recent takedowns with a small group of researchers who study and counter influence operations. We've continued to improve this *beta* platform in response to feedback from various research teams at the Digital Forensic Research Lab at the Atlantic Council, the Stanford Internet Observatory, the Australian Strategic Policy Institute, Graphika, and Cardiff University.

In the coming months, we'll be expanding this archive to more researchers around the world. Through this CrowdTangle-enabled interface, researchers — including our own — will be able to apply both quantitative and qualitative analysis to disrupted operations without the need to manually go through large spreadsheets or search for archived posts. We hope that being able to study the networks we've removed in a way that is as close to how they appeared on our platform as possible will help educate our global community about how best to spot these deceptive campaigns, including the signs of coordination and inauthenticity they present. We're looking forward to future research opportunities that this platform will spark and hope that it will help push industry standards forward on both the type and the format of information provided to scholars and OSINT researchers on security-related issues.

REMOVING AN ADVERSARIAL NETWORK IN ITALY AND FRANCE FOR BRIGADING

***What is [Brigading](#)?** We will remove any adversarial networks we find where people work together to mass comment, mass post or engage in other types of repetitive mass behaviors to harass others or silence them. Brigading activity can range from highly sophisticated intimidation operations to stifle dissent, to crude harassment campaigns to drown out opposing viewpoints.*

We removed a network of accounts that originated in Italy and France and targeted medical professionals, journalists, and elected officials with mass harassment. Our investigation linked this activity to an anti-vaccination conspiracy movement called V_V, publicly [reported](#) to engage in violent online and offline behaviors. The people behind this operation relied on a combination of authentic, duplicate and fake accounts to mass comment on posts from Pages, including news entities, and individuals to intimidate them and suppress their views.

While this network mass-harassed people on social media, including Facebook, YouTube, Twitter, and VKontakte, they apparently coordinated through Telegram in an attempt to evade detection. In their comments on social media, this group would typically include links to their Telegram channels. According to open source reporting, they would use Telegram to train members through videos, audio and live interviews how to circumvent detection and brigade people. Then, these accounts would flock to their target posts to leave dozens — and in some cases tens of thousands — of comments. In an apparent attempt to stay under the radar of content enforcement, they would only comment, not post, while altering words or using coded language. For example, in many posts, they would say “*Vaxcinati*” (translated as “those vaccinated”) where one letter is replaced. Notably, many of the accounts managed by each operator in this network had the same identifying number in their bio, likely to make it easier to keep track of who’s managing what.

In their comments, these accounts used the same text or manipulated images of their targets, including with superimposed swastika and other symbols. They would often call doctors, journalists and media “Nazi supporters” for promoting COVID vaccines, claiming that mandatory vaccination will lead to “healthcare dictatorship”.

The approach behind this group’s social media activity appeared to be two-fold. First, they sought to mass-harass individuals with pro-vaccination views into making their posts private or deleting them. Second, they tried to take advantage of popular Pages’ audiences to spread anti-vaccination misinformation through commenting at high volume. Over the course of this

network's activity on our platform, our automated and review systems enforced against their comments and accounts for various violations of our Community Standards, including hate speech, misinformation, incitement to violence, bullying and harassment. While we aren't banning all V_V content, we're continuing to monitor the situation and will take action if we find additional violations to prevent abuse on our platform and protect people using our services.

REMOVING AN ADVERSARIAL NETWORK IN VIETNAM FOR MASS REPORTING

***What is [Mass Reporting](#)?** We will remove any adversarial networks we find where people work together to mass-report an account or content to get it incorrectly taken down from our platform.*

We removed a network of accounts in Vietnam for violating our Inauthentic Behavior policy against mass reporting. They coordinated the targeting of activists and other people who publicly criticized the Vietnamese government and used false reports of various violations in an attempt to have these users removed from our platform. The people behind this activity relied primarily on authentic and duplicate accounts to submit hundreds — in some cases, thousands — of complaints against their targets through our abuse reporting flows.

Many operators also maintained fake accounts — some of which were detected and disabled by our automated systems — to pose as their targets so they could then report the legitimate accounts as fake. They would frequently change the gender and name of their fake accounts to resemble the target individual. Among the most common claims in this misleading reporting activity were complaints of impersonation, and to a much lesser extent inauthenticity. The network also advertised abusive services in their bios and constantly evolved their tactics in an attempt to evade detection.

NOVEMBER 2021: COORDINATED INAUTHENTIC BEHAVIOR REPORT

We're constantly working to find and stop coordinated campaigns that seek to manipulate public debate across our apps.

PURPOSE OF THIS REPORT

Over the past four years, we've shared our findings about [coordinated inauthentic behavior](#) we detect and remove from our platforms. As part of our regular CIB reports, we're sharing information about all networks we take down over the course of a month to make it easier for people to see the progress we're making in one place.

WHAT IS CIB?

We view CIB as coordinated efforts to manipulate public debate for a strategic goal where fake accounts are central to the operation. There are two types of these activities that we work to stop: 1) coordinated inauthentic behavior in the context of domestic, non-government campaigns and 2) coordinated inauthentic behavior on behalf of a foreign or government actor.

When we find campaigns that include groups of accounts and Pages seeking to mislead people about who they are and what they are doing while relying on fake accounts, we remove both inauthentic and authentic accounts, Pages and Groups directly involved in this activity.

CONTINUOUS ENFORCEMENT

We monitor for efforts to re-establish a presence on Facebook 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.

SUMMARY OF OCTOBER 2021 FINDINGS

We removed four networks — from Palestine, Poland, Belarus, and China. They all targeted audiences in multiple countries at once. This month, we're also sharing our internal research and analysis of one of the operations — a sprawling and unsuccessful network from China that targeted global English-speaking audiences in the United States and United Kingdom, and also Chinese-speaking audiences in Taiwan, Hong Kong, and Tibet. This deep-dive also includes, *for the first time*, specific threat indicators to facilitate further research by the open-source community into this COVID-19-focused activity across the internet.

(We will update the numbers as soon as the latest data becomes available)

- **Total number of Facebook accounts removed: 737**
- **Total number of Instagram accounts removed: 115**
- **Total number of Pages removed: 99**
- **Total number of Groups removed: 26**

NETWORKS REMOVED IN NOVEMBER 2021:

- 1. Palestine:** We removed 141 Facebook accounts, 79 Pages, 13 Groups and 21 Instagram accounts from the Gaza Strip in Palestine that primarily targeted people in Palestine, and to a much lesser extent in Egypt and Israel. We found this activity as part of our internal investigation into the suspected coordinated inauthentic behavior in the region and linked it to Hamas.
- 2. Poland:** We removed 31 Facebook accounts, four Groups, two Facebook Events and four Instagram accounts that we believe originated in Poland and targeted Belarus and Iraq. We found this activity as a result of our internal investigation into suspected coordinated inauthentic behavior in the region as we monitored the unfolding crisis at the border between Belarus and the EU. We moved quickly to complete the investigation and remove this network.
- 3. Belarus:** We removed 41 Facebook accounts, five Groups, and four Instagram accounts in Belarus that primarily targeted audiences in the Middle East and Europe. We found this activity as a result of our internal investigation into suspected CIB in the region as we monitored the ongoing crisis at the border between Belarus and the EU, and moved quickly to complete the investigation and remove this network. We linked it to the Belarusian KGB.
- 4. China:** We removed 524 Facebook accounts, 20 Pages, four Groups, and 86 accounts on Instagram. This network originated primarily in China and targeted global English-speaking audiences in the US and the UK, and also Chinese-speaking audiences in Taiwan, Hong Kong, and Tibet. We began looking into this activity after reviewing public reporting about the single fake account at the center of this operation. Our investigation found links to individuals in mainland China, including employees of Sichuan Silence Information Technology Co, Ltd (an information security firm) and individuals associated with Chinese state infrastructure companies based around the world.

01

We removed 141 Facebook accounts, 79 Pages, 13 Groups and 21 Instagram accounts for violating our policy against [coordinated inauthentic behavior](#). This network originated in the Gaza Strip in Palestine and primarily targeted people in Palestine, and to a much lesser extent in Egypt and Israel.

The people behind this activity used fake accounts to post and manage Groups and Pages. Some of these Pages claimed to be operated by news entities and communities from the West Bank, Israel, and Sinai in Egypt, while others purported to be independent news Pages in Palestine. These accounts claimed to be based in the target regions; many of them posed as young women in the West Bank or Sinai. Many of this network's accounts were already detected and disabled for being fake or other violations of our Community Standards.

The individuals behind this activity posted news stories, cartoons and memes primarily in Arabic about current events in the region, including the postponed Palestinian election, criticism of Israeli defense policy, Fatah and Mahmoud Abbas, and supportive commentary about Hamas.

We found this network as part of our internal investigation into the suspected coordinated inauthentic behavior in the region. Although the people behind it attempted to conceal their identities and coordination, our investigation found links to Hamas.

- *Presence on Facebook and Instagram:* 141 Facebook accounts, 79 Pages, 13 Groups and 21 Instagram accounts.
- *Followers:* About 407,000 accounts followed one or more of these Pages, around 2,000 people joined one or more of these Groups, and about 6,000 accounts followed one or more of these Instagram accounts.
- *Advertising:* Around \$21,000 in spending for ads on Facebook and Instagram paid for primarily in US dollars.

Below is a sample of the content posted by some of these Pages and accounts.



Translation

Page name: We Want Elections



Translation:

Page Name: Stay Aware

Caption and image overlay: Attention! The Israeli enemy is still impersonating "charities" as part of efforts to gather information and carry out its sabotage missions, as was evident during the infiltration of the Special Forces east of Khan Yunis.

Be careful with anonymous associations, and verify their identity.

#stay_aware

الإذاعة العبرية: الملك الأردني استدعى الرئيس عباس لتوبيخه

فلسطين 21:
كشفت الإذاعة العبرية صباح اليوم عن مصدر مطلع، أن الملك الأردني عبد الله الثاني استدعى رئيس السلطة محمود عباس من أجل توبيخه بسبب استخدام السلطة للتعنف المفرط والذي قد يؤدي لانهارها....
See more

Hebrew Radio: Jordanian King summoned President Abbas to rebuke him

Palestine 21:

Hebrew radio revealed this morning from a informed source that Jordanian King Abdullah II summoned President Mahmoud Abbas to rebuke him over using power for excessive violence that could lead to its collapse.

King Abdullah warned of the possibility of power collapse and its negative impact on the stability of the region, and took responsibility for the deterioration of the situation for the security leaders accompanied by President Major General Majid Faraj and Minister Hussein Al Sheikh.

The Jordanian King sees continuing power important in facing plans to settle Palestinians east of the Jordan River, a Hebrew source says.

President Abbas' visit to Jordan comes following the escalation of events in the Bank following the power assassination of opposition political activist Nizar Banat.

[Hide Translation](#) - [Rate this translation](#)



Translation

Page name: Palestine 21

02

We removed 31 Facebook accounts, four Groups, two Facebook Events and four Instagram accounts for violating our policy against [coordinated inauthentic behavior](#). We believe this network originated in Poland and targeted Belarus and Iraq.

The core of this activity began in September 2021. The people behind it used exclusively fake accounts — many of which were already detected and disabled by our automated systems — to pose as migrants from the Middle East posting about the border crisis between Belarus and the European Union. Nearly all these accounts were created in recent months. One of the fake accounts, with a profile photo likely generated using artificial intelligence techniques like generative adversarial networks (GAN), planned a protest event in Minsk that it advertised on Facebook. Local media publicly reported the planning of this event. We removed it in November as part of disrupting this operation.

This network appeared to operate across multiple platforms, including by reposting YouTube videos on Facebook, to dissuade migrants from entering the EU. The language and narratives were specifically tailored for particular migrant groups and the fictitious personas posting them. These fake personas claimed to be sharing their own negative experiences of trying to get from Belarus to Poland and posted about migrants' difficult lives in Europe. They also posted about Poland's strict anti-migrant policies and anti-migrant neo-Nazi activity in Poland. They also shared links to news articles criticizing the Belarusian government's handling of the border crisis and off-platform videos alleging migrant abuse in Europe.

We found this activity as a result of our internal investigation into suspected coordinated inauthentic behavior in the region as we monitored the crisis at the border, and moved quickly to complete the investigation and remove this network.


- *Presence on Facebook and Instagram:* 31 Facebook accounts, four Groups and four Instagram accounts.
- *Followers:* Around 600 people joined one or more of these Groups, and about 10 accounts followed one or more of these Instagram accounts.

- *Events:* two events were planned by these Pages. Up to 90 people expressed interest in at least one of these events. We cannot confirm whether any of these events actually occurred.

Below is a sample of the content posted by some of these Pages and accounts.

shared a link.
November 19 at 8:36 AM · 🌐

تذكر حول مظاهراتنا! يوما بعد يوم يعرف المزيد من الناس عن مشاكلنا حتى الناس من الغرب.
Remembering about our demonstration! Day by day more people know about our problems even the people from the west.
<https://twitter.com/franakviac.../status/1461450122039107590>
Hide Translation · Rate this translation



FRIDAY, 26 NOVEMBER 2021 AT 13:00 UTC+02

The demonstration for refugees support ⓘ

TWITTER.COM
Franak Viačorka on Twitter
"Unexpectedly, migrants announced a peaceful rally in the center of Minsk against Luk..."

1 · 3 Comments

November 16 at 9:03 AM · 🌐

I can't believe what I found on twitter...
THERE IS A PROOF, that poor people are forced and manipulate!!!
according to my last post..
Belarusians beat immigrants
🤔🤔🤔🤔🤔
WARNING: it's heartbreaking



0:03 / 0:16

كروپی كوردانی ئه‌وروپا
Nov 14 2021 5:23pm UTC+00:00

According to the post of Hama Gian last night, the Belarusian soldiers took a few of the Kurdish men and forced them to cut the fence otherwise they would hit them and all their relatives who were with them. Please stand and don't be afraid. They used us to fight for them in their little war with the EU. Now they treating us to death! What will happen next ?

Undo

03

We removed 41 Facebook accounts, five Groups, and four Instagram accounts for violating our policy against [coordinated inauthentic behavior](#). This activity originated in Belarus and primarily targeted audiences in the Middle East and Europe.

The core of this activity began in October 2021, with some accounts created as recently as mid-November. The people behind it used newly-created fake accounts — many of which were detected and disabled by our automated systems soon after creation — to pose as journalists and activists from the European Union, particularly Poland and Lithuania. Some of the accounts used profile photos likely generated using artificial intelligence techniques like generative adversarial networks (GAN). These fictitious personas posted criticism of Poland in English, Polish, and Kurdish, including pictures and videos about Polish border guards allegedly violating migrants' rights, and compared Poland's treatment of migrants against other countries'. They also posted to Groups focused on the welfare of migrants in Europe. A few accounts posted in Russian about relations between Belarus and the Baltic States.

We found this activity as a result of our internal investigation into suspected coordinated inauthentic behavior in the region as we monitored the border crisis, and moved quickly to complete the investigation and remove this network. Although the people behind it attempted to conceal their identities and coordination, our investigation found links to the Belarusian KGB.

- *Presence on Facebook and Instagram:* 41 Facebook accounts, five Groups and four Instagram accounts.
- *Followers:* Less than 1,400 people joined one or more of these Groups, and less than 200 accounts followed one or more of these Instagram accounts.

Below is a sample of the content posted by some of these accounts.



Oct 11 2021 9:58am

Polscy żołnierze strzelają w powietrze i biją uchodźców pałkami 8 października na jednym z odcinków granicy polsko-białoruskiej białoruski pogranicznik usłyszał odgłosy strzałów i przybył na miejsce zdarzenia. Na terenie Polski w pobliżu granicy znajdowała się duża grupa uchodźców otoczonych przez polskich żołnierzy. Cudzoziemcy krzyczeli i prosili o zaprzestanie przemocy. W odpowiedzi na zgodne z prawem prośby uchodźców o przyznanie im prawa do ochrony, polskie wojsko wystrzeliło w powietrze, użyło pałek przeciwko uchodźcom i zażądało udania się na Białoruś. Mimo zastraszania bronią i użyciem siły fizycznej cała grupa odmówiła przekroczenia granicy z Białorusią. Przedstawiciele polskiej Straży Granicznej starają się ukrywać oczywiste fakty użycia broni w celu wypędzenia uchodźców i celowo składać fałszywe zeznania, publikując informacje o odgłosach strzałów rzekomo pochodzących ze strony białoruskiej. Polska coraz bardziej zniekształca wydarzenia na granicy, bezpodstawnie oskarżając stronę białoruską, tym samym starając się odwrócić uwagę od nielegalnych działań polskich sił bezpieczeństwa w stosunku do uchodźców. Film jest prezentowany na stronie internetowej Państwowego Komitetu Granicznego Republiki Białorusi.

[Translate](#)



Translation

Polish soldiers shoot in the air and beat refugees with clubs On October 8, at one of the sections of the Polish-Belarusian border, a Belarusian border guard heard the sound of shots and arrived at the scene. In Poland, near the border, there was a large group of refugees surrounded by Polish soldiers. The foreigners shouted and asked for the violence to stop. In response to the refugees' lawful requests to grant them the right of protection, the Polish military fired into the air, used truncheons against the refugees, and ordered them to go to Belarus. Despite the intimidation with weapons and the use of physical force, the entire group refused to cross the border with Belarus. Representatives of the Polish Border Guard are trying to hide the obvious facts of the use of weapons to expel refugees and deliberately give false testimony by publishing information

about the sounds of shots allegedly coming from the Belarusian side. Poland distorts the events on the border more and more, unjustifiably accusing the Belarusian side, thus trying to divert attention from the illegal activities of Polish security forces in relation to refugees. The film is presented on the website of the State Border Committee of the Republic of Belarus.



Nov 25 2021 8:53am

The EU lies! On November 23, the European Commission decided to allocate 3.5 million euros to support the voluntary return of migrants from Belarus to their countries of origin. Earlier 700 thousand euros were allocated for humanitarian assistance to vulnerable refugees and migrants who found themselves in Belarus. Everything looks beautiful in words, but the EU assistance ended up after paying for one flight from Minsk to Baghdad. The next flight supposed to take migrants from Minsk to Iraq on November 25, was canceled by the decision of Iraqi Airways. The reason for the cancellation of the flight was the EU's refusal to pay for the flight. Where did 3.5 million euros go so quickly?

Translate



Nov 16 2021 2:24pm

Germany is ready to accept refugees. Instead of allowing refugees to pass through and giving them a humanitarian corridor, Poland is pouring water cannons on refugees and poisoning them with gas and grenades.

Translate



2

04

IN DEPTH RESEARCH & ANALYSIS

THE SWISS BIOLOGIST THAT NEVER WAS

A Chinese influence operation focused on COVID-19

By Ben Nimmo, Global IO Threat Intelligence Lead and the IO Threat Intelligence Team

EXECUTIVE SUMMARY:

On July 24, 2021, someone posing as a Swiss biologist named Wilson Edwards claimed, on Facebook and Twitter, that the United States was putting pressure on World Health Organization scientists studying the origins of COVID-19 in an attempt to blame the virus on China. Within 48 hours, hundreds of social media accounts around the world had picked up on the story. Within a week, Chinese state media including the [Global Times](#) and [People's Daily](#) were running headlines about the alleged US “intimidation.”

On August 10, the Swiss Embassy in Beijing [announced](#) that there was no record of any Swiss citizen by that name. The same day, we investigated and removed the Facebook account as fake. It had been created on July 24, less than 12 hours before it started posting about the coronavirus pandemic.

In essence, this campaign was a hall of mirrors, endlessly reflecting a single fake persona. Our investigation uncovered that almost the entire initial spread of the “Wilson Edwards” story on our platform was inauthentic — the work of a multi-pronged, largely unsuccessful influence operation that originated in China. The operation brought together the original fake account, several hundred additional inauthentic accounts and a cluster of authentic accounts, including those that belonged to employees of Chinese state infrastructure companies across four continents. Outside these clusters, only a handful of real people engaged with the operation’s content.

Although the people behind this network attempted to conceal their identities and coordination, our investigation found links to individuals in mainland China, including employees of Sichuan Silence Information Technology Co, Ltd (an information security firm) and individuals associated with Chinese state infrastructure companies located around the world. This is the first time we have observed an operation that included a coordinated cluster of state employees to amplify itself in this way.

Finally, and separately from these clusters, our investigation also found that a number of Chinese government officials began interacting with the operation's content less than an hour after it first posted, and up to 12 hours before the amplification clusters began liking and sharing it.

We shared our findings with industry peers, policymakers, law enforcement and independent researchers. To inform further research by the open-source community into this and similar activity across the internet, we are also sharing a set of IO indicators at the end of this report.

TAKEDOWN BY THE NUMBERS

- *Presence on Facebook and Instagram:* 524 Facebook accounts, 20 Pages, four Groups, and 86 accounts on Instagram.
 - *Followers:* About 72,000 accounts followed one or more of these Pages, about 10 accounts followed one or more of these Groups, and about 2,000 accounts followed one or more of these Instagram accounts. These figures reflect the following of all the Pages connected to this network, including spammy Pages that were not used in this particular campaign or for political posting. Only one Page with under 100 followers played an active role in the operation by sharing the same links as the rest of the accounts.
 - *Advertising:* Less than \$5,000 in spending for ads on Facebook and Instagram paid for primarily in US dollars.
-

The fake biologist

The operation began on July 24, 2021, with the creation of a fake persona called “Wilson Edwards” claiming to be a Swiss biologist, two days after China reportedly [rejected](#) a World Health Organization plan for the second phase of a study into the origins of COVID-19.

This account was created at 05:49 UTC. At 15:53 UTC — about ten hours after its birth — it posted a lengthy text which claimed that “WHO sources and a number of fellow researchers” had complained of “enormous pressure and even intimidation” from the United States over the WHO’s plan for a renewed COVID origins probe. It posted the identical text three more times within the next hour, then stopped posting, never to resume. The same day, a Twitter account with the same name and profile picture was created, tweeted a few times including the same text, and fell silent.

Although the persona was newly created, the operators took steps to conceal its origin by using VPN infrastructure and gave it a rounded personality. Before launching its main, WHO-focused post, the Facebook account posted about dieting, a link to the Facebook COVID-19 Information Center, and the Olympics. On Twitter, its first tweet read “Pray” and the second was about COVID vaccination passports in Northern Ireland.

This persona appeared to target audiences who were already focused on the World Health Organization by posting in reply to the WHO’s official social media posts. On Facebook, they replied to two different posts by the WHO’s Page. On Twitter, they replied to tweets by the WHO’s Western Pacific office, the WHO’s main account, WHO Director General, and a fan account dedicated to Dr. Anthony Fauci, the Chief Medical Advisor to the US President. These efforts failed to attract any noticeable authentic engagement.

Inauthentic amplifiers

Once “Wilson Edwards” posted, the operation proceeded to amplify “him” in three waves of inauthentic amplification. None of them translated into any authentic engagement, based on our assessment. This is consistent with what we’ve seen in our research of covert influence operations over the past four years: we haven’t seen successful IO campaigns built on fake engagement tactics. Unlike elaborate fictitious personas that put work into building authentic communities to influence them, the content liked by these crude fake accounts would typically be only seen by their “fake friends.”

First, soon after the main post claiming the US was putting pressure on WHO scientists, half a dozen fake accounts shared it. Three of them were created that same day; all had technical links to the “Wilson Edwards” account and to individuals at the information security firm Sichuan Silence Information Technology in China. These accounts mostly posed as Westerners. They shared Edwards’ post into two London-focused groups (“London Friends” and “London Marketplace”). None of their posts received any engagement. Around the same time, a batch of fake Twitter accounts began liking and retweeting the equivalent tweet.

Second, in the following hours, some 200 inauthentic Facebook accounts “liked” the post. The great majority of these accounts were created in batches in early 2021. Many had copied their profile pictures from commonly available online sources, while some had profile photos likely generated using machine learning techniques like generative adversarial networks (GAN), a technique we have observed with increasing frequency since December 2019. Apart from liking this post, they were barely active, with typically a handful of posts or likes of non-political content each. This fake engagement was primitive in nature and didn’t result in any traction for the post among authentic communities.



Image

Profile picture of one of the batch-created fake accounts that liked the “Wilson Edwards” post. The photo appeared to be GAN-generated.

Third, starting at 10:55 UTC on the morning of July 25 (the day after the Edwards account posted), around 100 fake accounts began posting a link to the “biologist’s” main WHO-focused post. This link was in mobile form (beginning with m[.]facebook[.]com), which is typically generated when someone views a post in a mobile browser and copies the URL from there. The fact that all these accounts posted the mobile link as a text string on their Facebook timelines is somewhat unusual: none of them shared the post in the typical way, by clicking “share”, or by posting the standard, non-mobile form of the URL.

Their posting behavior that day was unusual in another way as well: within minutes of sharing the mobile link to the “Wilson Edwards” post, each account also posted a link to an article on Yahoo News, originally taken from the Washington Examiner, headlined, “Fauci and top Wuhan scientist cite same study to cast doubt on COVID lab leak”. None of the accounts posted anything else that day.

The fact that they all both posted the mobile URL as a text string and did so in immediate combination with the Yahoo News / Washington Examiner link might suggest a centralized distribution of the content which they all copy-pasted on their timelines.

These accounts were created between February and June 2019. Many had profile pictures of cartoons, animals or food. A few had photos of young women — also likely copied from the internet. They only became active in late 2020 or early 2021 and behaved similarly by posting links to various news articles and social media posts, particularly from Chinese state media. Typically, they did this at the same time and in the same order. None of these accounts posted anything except links (i.e. no captions or comments added to the links in their posts). Just like the previous two waves of amplification, these posts fail in gaining any authentic attention.



Image

Screenshots of the posts by two fake accounts sharing a link to the news article with a cartoon on the US response to COVID-19. The two accounts shared this article as a link in the same minute.



A Covert Chorus

One of the most interesting and unique aspects of this operation appeared on the morning of July 25. At the same time as the fake accounts were beginning their amplification efforts, another cluster of accounts began posting the exact same two links to the mobile version of the “Wilson Edwards” post and the Yahoo News / Washington Examiner article, as the fake accounts we discussed earlier. While some of these accounts were fake or duplicate, many were authentic.

The majority of the authentic accounts belonged to employees of Chinese state infrastructure companies in over 20 countries, including Algeria, Brazil, Hong Kong, Indonesia, Kazakhstan, Kenya, Nepal, the Philippines, Saudi Arabia and Tanzania. They represented sectors that included civil engineering, power generation, telecoms and transport. This global cluster appeared to similarly operate on Twitter where they too posted the same two links.

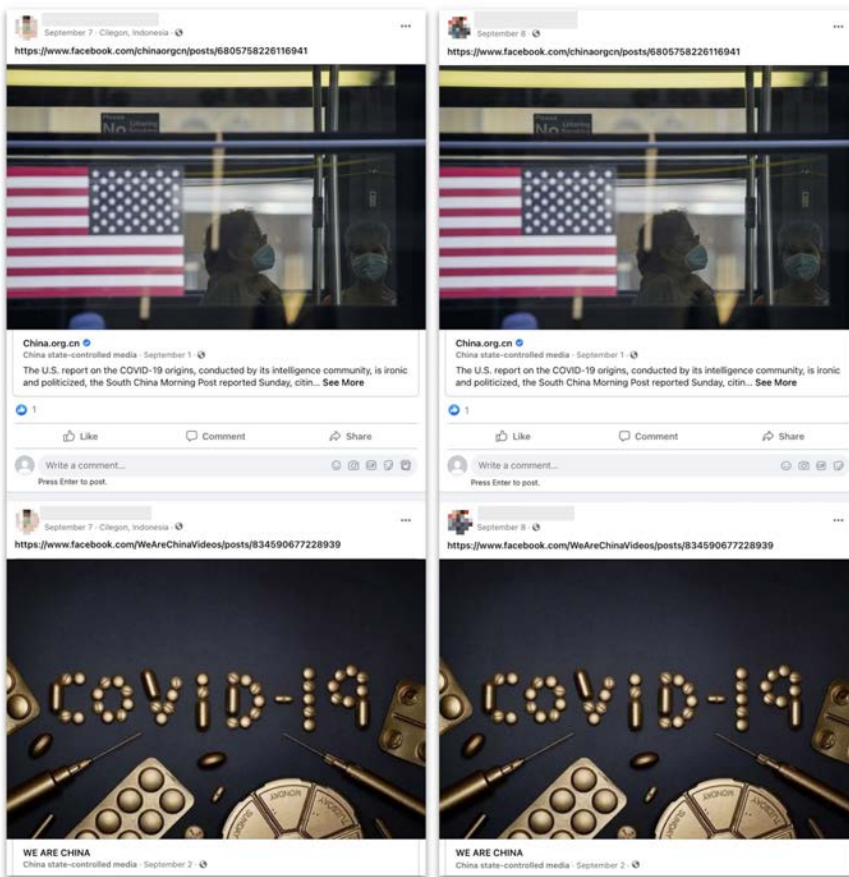
Image

Posts made from Iraq (top) and Kenya (bottom) on July 25, 2021. In each case, the lower post contains the link to the Yahoo News/Washington Examiner article. The upper post contains the mobile link to the “Wilson Edwards” post. Each account posted the two links within a few minutes.



Notably, this behavior was not unusual for many of these authentic and duplicate accounts operated from around the world. Before and after the July operation, they all repeatedly posted identical pairs of URLs to news articles and social-media posts that praised China or criticized its critics, without any accompanying comments (different link pairs from the Wilson Edwards campaign).

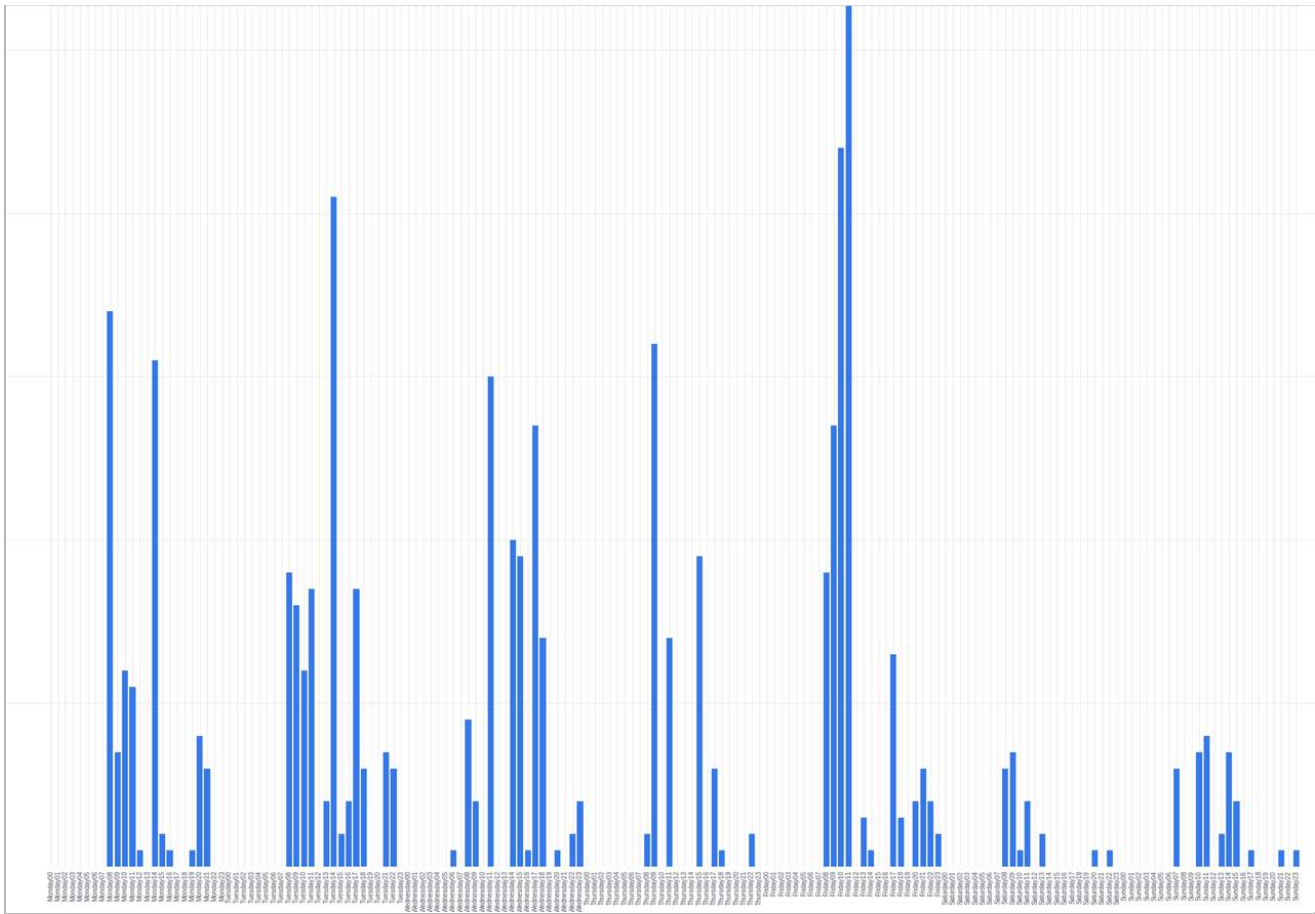
This general behavior resembled that of the inauthentic amplifiers, but the two clusters usually posted different combinations of links. We have listed some of them in the Appendix to enable further research by the open-source community into this network's activity across the internet.



Image

Posts made from Indonesia (left) and Kenya (right) sharing the same links in the same order. Note that the text is limited to the URLs themselves, with no commentary.

Some of the fake accounts in this cluster were named after the companies the operators behind them worked for, essentially using user profiles as if they were Pages. Many accounts in this global cluster — whether authentic or not — posted during working hours, Monday through Friday, in a very consistent pattern.



An example of a graph that shows posting behavior by accounts from Algeria from 8AM to 4PM, with a heavier activity on Friday mornings.

On a very few occasions, the people in this worldwide network shared posts that exposed coordination amongst them. On July 26, an account in Indonesia shared our typical combination of the mobile link to the “Wilson Edwards” post and the link to the Yahoo News article as a single post, together with instructions in Indonesian and Chinese on how to amplify them. The Chinese instructions included details on how and when to report back on reactions, with an explicit focus on “overseas social media accounts”. This person made the post almost 24 hours *after* the authentic network had begun sharing the two URLs.



Image

The post by the Indonesian account, sharing the “Wilson Edwards” and Yahoo links.

Translation

Indonesian: Good morning and greetings to all colleagues, help to share and click the link below

Chinese: Leaders and colleagues: Please link and forward the following content on overseas social media accounts, and feedback and disseminate by 15:00 tomorrow (July 26) Circumstances (including but not limited to: dissemination of data, highlight interaction, big V forwarding, etc.), thank you~: 1. Yahoo News published "Fauci and top Wuhan scientist cite same study to cast doubt on COVID lab leak" push link:

<https://news.yahoo.com/fauci-top-wuhan-scientist-cite-173900362.html> 2. Wilson Edwards post "WHO is conducting virus traceability research" Push link:

https://m.facebook.com/story.php?story_fbid=101513595554063&id=100070862673911

Completely separately from the Wilson Edwards operation, on September 27, someone else in the network — this time based in Singapore — made two posts in the same minute, each of them containing one link to an English-language article, plus a brief Chinese text. One was to a China Daily story about a Chinese diplomat rejecting a US report on the origins of COVID-19; the other linked to an article in the Oklahoma Star about Chinese grape exports. The former post was accompanied by a set of instructions, while the latter was accompanied by a readout of how many times the story had been re-published by media organizations worldwide.



Image

Two posts by the account in Singapore.

Translation:

Upper post: Broadcast "Global Connection[A 'Purple Business Card' for External Communication". After the manuscript was broadcast on the English Internet dedicated line, it was adopted by 77 domestic and foreign media including asianpacificstar.com and buffalobreeze.com.

Lower post: Continue to do a good job in the struggle and guidance of public opinion on the traceability of the epidemic. The China Daily website and the client published a poster "Indonesian Ambassador: "Intelligence Traceability" can be stopped".

A few hours later, a Page in the Philippines — the only Page we found to have played a direct role in the Wilson Edwards operation — posted the same exact English URLs and the instructions in Chinese. This time they were presented as a numbered list in a single post. The admin of the Philippines Page was not connected to the account in Singapore. The fact that they used the same text with the same combination of links suggests that the Singapore account and the Philippines Page were likely both copying their content, including the instructions, from a common source.



Image

Post by the Page operated from the Philippines.

Translation:

1. Broadcast "Global Connection[A "Purple Business Card" for External Communication". After the manuscript was broadcast on the English Internet dedicated line, it was adopted by 77 domestic and foreign media including [http://xn--asiapacificstar-tk96b\[.\]com/](http://xn--asiapacificstar-tk96b[.]com/) and [buffalobreeze\[.\]com](http://www.oklahomastar.com/).
2. Continue to do a good job in the struggle and guidance of public opinion on the traceability of the epidemic. The China Daily website and the client published a poster "Indonesian Ambassador: "Intelligence Traceability" can be stopped".

With this cluster relying on the authentic accounts of the Chinese state employees abroad showing strong signals of coordination, this operation and the tactics it used offers an important area for future research into the ways coordination across 20 countries might work.

It's important to note however that the reach of this operation was very limited and primarily manifested in the fake biologist's claims getting picked up by the Chinese state media and then quickly debunked by the international community, including the Swiss embassy in Beijing. Typical URL shares by this network gained single-digit engagements at most, and few if any comments.

Influence experiments

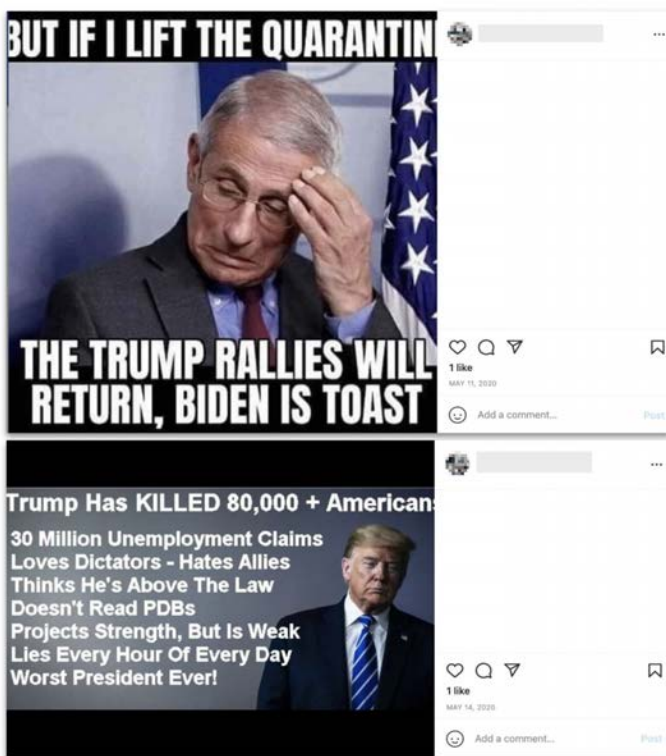
The cluster of fake accounts that were directly connected to the "Wilson Edwards" persona and individuals associated with the information security firm Silence in China appears to have unsuccessfully experimented with other influence operations in preceding years.

These attempts were typically small-scale and of negligible impact, with clusters of around half a dozen accounts posting about political issues in different countries for a few weeks or months, and then falling silent again. They also ran a handful of Pages we removed for spam that posted

non-political content — these accounted for the great majority of Page likes we reported in this write-up, the largest of which were detected and disabled by our automated systems.

The earliest activity that we have been able to detect came in early 2018. Fake accounts amplified other people’s posts in Chinese, including about Hong Kong and Taiwan. It usually lasted a few months and attracted almost no engagement.

A second try began in mid-2020, in English, and focused on US domestic politics and foreign relations. One Instagram account posted about then-President Trump, with a mixture of both critical and supportive posts. A pair of Facebook accounts posted about the US’ struggles to contain COVID-19 in both English and Chinese. This activity lasted from April through July 2020, and then fell silent. None of these posts gained significant engagement. This may have been an experimental foray into the English-speaking world and did not appear to be a full-scale influence attempt.



Image

Posts by one of the fake Instagram accounts in May 2020, with memes about former president Trump. Each post only received one like.

Of all this network’s posts, only the one by “Wilson Edwards” attracted any attention, and that was due to the Chinese state media.

APPENDIX: IO INDICATORS

This operation was unusual for the way in which different clusters of accounts repeatedly shared distinctive combinations of links to a range of articles across the internet — usually without any other text. These links typically came in pairs (occasionally threes); each account typically posted the links within 1-2 minutes of each other. The cluster of inauthentic amplifiers and the cluster of mainly authentic amplifiers both behaved in this way, but the two clusters typically shared different combinations of links.

These combinations of links were unique enough to be used as signals to surface other potential activity across the internet. Caution should be exercised in this analysis though: content signals alone are not enough to attribute particular activity to the operation with confidence, and should always be accompanied by detailed behavioral analysis. These pairs of links might provide a way to surface possible associated accounts across the internet for further analysis.

We present them here as potential future research areas by the open-source community:

1. Link pairs posted by the inauthentic amplifiers

Characteristics of the cluster: Typically, accounts were created between February and June, 2019. Many had profile pictures of cartoons, animals or food. A few had photos of young women as their profile pictures: these appear to have been copied from publicly available online sources. They usually claimed in their bios to live in South East Asia, particularly in Indonesia, while most had Western names.

1. [https://www\[.\]globaltimes.cn/page/202109/1235121.shtml](https://www[.]globaltimes.cn/page/202109/1235121.shtml) + [https://www\[.\]globaltimes.cn/page/202109/1235160.shtml](https://www[.]globaltimes.cn/page/202109/1235160.shtml)
2. [https://www\[.\]facebook.com/PDInternational/posts/405794314448568](https://www[.]facebook.com/PDInternational/posts/405794314448568) + [https://www\[.\]facebook.com/PDInternational/posts/405797291114937](https://www[.]facebook.com/PDInternational/posts/405797291114937)
3. [https://epaper\[.\]chinadaily.com.cn/a/202109/06/WS613559bca3106abb319fd491.html](https://epaper[.]chinadaily.com.cn/a/202109/06/WS613559bca3106abb319fd491.html) + [https://foto\[.\]agerpres.ro/foto/detaliu/14948513](https://foto[.]agerpres.ro/foto/detaliu/14948513)
4. [https://www\[.\]facebook.com/WeAreChinaVideos/posts/833409710680369](https://www[.]facebook.com/WeAreChinaVideos/posts/833409710680369) + [https://www\[.\]facebook.com/chinaorgcn/posts/6796093433750087](https://www[.]facebook.com/chinaorgcn/posts/6796093433750087)
5. [https://www\[.\]facebook.com/chinaorgcn/posts/6763957270297037](https://www[.]facebook.com/chinaorgcn/posts/6763957270297037) + [https://www\[.\]facebook.com/169799706487474/posts/2439820612818694/](https://www[.]facebook.com/169799706487474/posts/2439820612818694/)
6. [https://www\[.\]facebook.com/XinhuaNewsAgency/videos/1493807660955350/](https://www[.]facebook.com/XinhuaNewsAgency/videos/1493807660955350/) + [https://www\[.\]facebook.com/globaltimesnews/posts/4353033208110879](https://www[.]facebook.com/globaltimesnews/posts/4353033208110879)

7. http://www.xinhuanet.com/english/2021-07/26/c_1310086477.htm + <https://news.cgtn.com/news/2021-07-24/Uncle-Sam-s-selective-vision-on-COVID-19-origin-tracing-128eFp0PIxa/index.html>
8. https://m.facebook.com/story.php?story_fbid=101513595554063&id=100070862673911 + <https://news.yahoo.com/fauci-top-wuhan-scientist-cite-173900362.html>

Links pairs posted by the primarily authentic cluster

Characteristics of the cluster: Typically, these accounts belonged to people who self-identified in their bio as employees of Chinese state companies around the world. They usually posted many of the below pairs of links over a period of several months, hence one-off posting of these link pairs is insufficient to confirm the connection.

1. <https://www.facebook.com/PDInternational/posts/432459745115358> + <http://covid-19.chinadaily.com.cn/a/202110/25/WS61768494a310cdd39bc71249.html>
2. <http://www.chinadaily.com.cn/a/202110/20/WS616f4945a310cdd39bc6fecc.html> + <https://www.facebook.com/191347651290/posts/10159799898396291/>
3. <http://www.chinadaily.com.cn/a/202109/26/WS614fa2eca310cdd39bc6b7f3.html> + <https://www.oklahomastar.com/news/271295967/globalink--grapes-and-wine-the-purple-business-cards-of-ningxia>
4. <https://www.facebook.com/223495844457800/posts/2149115245229174/> + <https://www.facebook.com/XinhuaNewsAgency/videos/1218947891906788/> + <https://foto.jagerpres.ro/foto/detaliu/14967277>
5. <https://www.facebook.com/chinaorgcn/posts/6805758226116941> + <https://www.facebook.com/WeAreChinaVideos/posts/834590677228939>
6. <https://www.facebook.com/cctvcom/posts/10159985970034759> + <https://www.facebook.com/chinaorgcn/posts/6786171451408952>
7. <https://www.facebook.com/watch/?v=531342138203048> + <https://twitter.com/globaltimesnews/status/1427875994484940803>
8. <https://twitter.com/XHNews/status/1425767006209331208> + <https://www.facebook.com/chinadaily/photos/a.195840701290/10159676616971291/>
9. <https://business.facebook.com/echinanews/videos/824651808240751> + <https://www.facebook.com/chinaorgcn/posts/6674030699289695>
10. <https://www.facebook.com/globaltimesnews/posts/4330165013731032> + <https://www.facebook.com/globaltimesnews/posts/4331482713599262>
11. <https://twitter.com/globaltimesnews/status/1421888456930721793> + <https://twitter.com/ChinaDaily/status/1422116272372785156?s=20>
12. http://www.xinhuanet.com/english/2021-07/27/c_1310090195.htm + <https://www.thecitizen.co.tz/tanzania/oped/-depoliticising-covid-19-in-the-context-of-china-and-the-west-3488198>

13. [https://m\[.\]facebook.com/story.php?story_fbid=101513595554063&id=100070862673911](https://m[.]facebook.com/story.php?story_fbid=101513595554063&id=100070862673911) + [https://news\[.\]yahoo.com/fauci-top-wuhan-scientist-cite-173900362.html](https://news[.]yahoo.com/fauci-top-wuhan-scientist-cite-173900362.html)
14. [https://mp\[.\]weixin.qq.com/s/80Qy6j3sb61nX1z-Qf0pXQ](https://mp[.]weixin.qq.com/s/80Qy6j3sb61nX1z-Qf0pXQ) + [https://www\[.\]politico.com/news/2021/07/21/china-covid-coronavirus-origin-500523](https://www[.]politico.com/news/2021/07/21/china-covid-coronavirus-origin-500523)