SEPTEMBER 2022

DETAILED REPORT

Taking down coordinated inauthentic behavior from Russia and China

Ben Nimmo, Global Threat Intelligence Lead
Mike Torrey, Security Engineer

Meta

TABLE OF CONTENTS

PURPOSE OF THIS REPORT

Our public threat reporting began about five years ago when we first shared our findings about coordinated inauthentic behavior (CIB). In today's report, in addition to sharing our analysis and threat research, we're also publishing threat indicators to contribute to the efforts by the security community to detect and counter malicious activity elsewhere on the internet. (See Appendix).

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

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

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

KEY TAKEAWAYS

- We took down two unconnected networks in China and Russia for violating our policy against coordinated inauthentic behavior.
- The Chinese-origin influence operation targeted primarily the US and the Czech Republic. While small in size, it ran across Facebook, Instagram, Twitter, and also two petition platforms in Czechia. This was the first Chinese network we disrupted that focused on US domestic politics ahead of the midterm elections and Czechia's foreign policy toward China and Ukraine.
- The Russian network targeted primarily Germany, France, Italy, Ukraine and the UK, with narratives focused on the war in Ukraine and its impact in Europe. The largest and most complex Russian operation we've disrupted since the war in Ukraine began, it ran a sprawling network of over 60 websites impersonating news organizations, as well as accounts on Facebook, Instagram, YouTube, Telegram, Twitter, Change.org and Avaaz, and even LiveJournal.
- We shared information with our peers at tech companies, security researchers, governments and law enforcement so they too can take appropriate action. At the end of this report, we're also including threat indicators to help the security community detect and counter malicious activity elsewhere on the internet (See Appendix).

01

China

EXECUTIVE SUMMARY:

We took down a small network that originated in China and targeted the United States, the Czech Republic and, to a lesser extent, Chinese- and French-speaking audiences around the world. It included four, largely separate and short-lived efforts, each focused on a particular audience at different times between the Fall of 2021 and 2022. In the United States, they targeted people on both sides of the political spectrum. In Czechia, this activity focused on criticizing the state's support of Ukraine, its impact on the Czech economy, and calling for the government to avoid antagonizing China. Each cluster of accounts — around half a dozen each — posted content at low volumes during working hours in China rather than when their target audiences would typically be awake. Only a few people engaged with it and some of those who did called it out as fake. Our automated systems took down a number of accounts and Pages for various community standards violations, including impersonation and inauthenticity.

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

TAKEDOWN BY THE NUMBERS

- *Presence on Facebook and Instagram:* 81 Facebook accounts, eight Pages, one Group and two accounts on Instagram.
- *Followers:* About 20 accounts followed one or more of these Pages, around 250 accounts joined one or more of these Groups and less than 10 accounts followed one or more of these Instagram accounts.

FOUR KEY EFFORTS

This network's activity was split into four clusters. The first, mostly in Chinese, posted mainly about geopolitical issues, criticizing the US. The second and third clusters, mainly in English, targeted both sides of the political spectrum in the US. The fourth, in Czech, targeted the Czech Republic. As the network's targeting shifted over time, we also saw a shift in tactics. During the first two efforts, the network ran fake accounts that posted and shared comments and memes. The third US-focused cluster added Pages and political hashtags. On Facebook, these hashtags were used almost exclusively by this network, rather than authentic communities. On Twitter, these hashtags appeared to have been used by a handful of accounts as well. The final cluster also ran petitions on Czech websites.

Of all these efforts, only the Czech-focused cluster saw some engagement, specifically a few hundred signatures on its petitions on domestic petition websites. The US-focused clusters saw minimal reactions across their posts into US Groups. For example, two memes about President Joe Biden and Senator Marco Rubio received one engagement each (illustrated below). None of the operation's US-facing Pages had more than a handful of followers. Of the US-focused hashtags, only two were ever shared by operation accounts, and the third was shared by a small handful of real people, independent of this campaign.

Top image

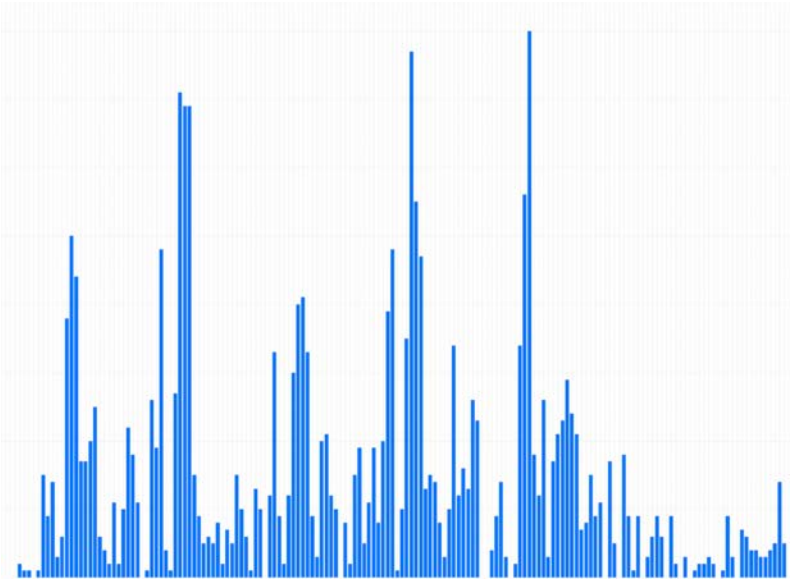
Meme posted by one of the operation's Cluster 2 accounts, April 18, 2022.

Bottom image

Meme posted by one of the operation's Cluster 3 accounts, August 2, 2022.

This operation failed to gain following or engagement from authentic communities. First, this activity was very sporadic in nature: they ran a very small number of accounts in each cluster, only kept them going for a few weeks, and posted infrequently. For example, some accounts shared the same post into a few Groups on one day, and then didn't post for a week. What they did post included linguistic errors: "I can't live in an America on regression !"

Second, these accounts largely stuck to a shift pattern that coincided with a nine-to-five, Monday-to-Friday work schedule during working hours in China — 12 hours ahead of Florida and six hours ahead of Prague. They appear to have had a substantial lunch break, and a much lower level of posting during weekends. This meant that the operation was mostly posting when Americans were sleeping. For example, both memes illustrated above were posted around 4am Eastern Standard Time.



Image

Time pattern for the operation's posts, set to Beijing time, Monday to Sunday.

CLUSTER NUMBER ONE

Key takeaways:

- Posted from November 2021 to September 2022
- Posted primarily in Chinese
- Fake accounts had female names in English but male profile photos
- Themes: criticism of the US and its foreign policies, surveillance and alleged cyber attacks.

In late November 2021, the people behind this activity began running a batch of fake accounts that first shared long text posts in Chinese and then added memes that accused the United States of surveillance and cyber attacks against China. These posts were shared every few weeks by accounts that appeared to invest the least in developing fictitious personas. In fact, even though they posted in Chinese, these accounts had female English names while their profile pictures were

of men in formal attire. Few of their posts received any engagement. This cluster was the largest and least sophisticated part of the operation.

Image

A post by one of the accounts in the Chinese-language *cluster number one.*

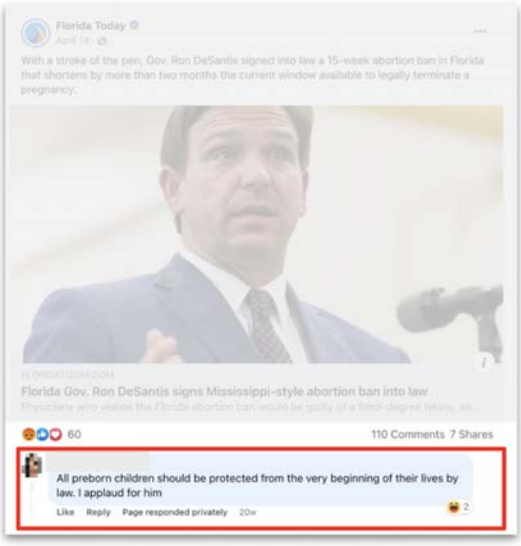
CLUSTER NUMBER TWO

Key takeaways:

- Posted from March to April 2022
- Posted primarily in English and to a much lesser extent in Chinese and French
- Fake accounts posed mainly as conservative Americans
- Themes: pro-gun rights and anti-abortion rights in the US; claims of the US-run bioweapons labs in Ukraine; and criticism of President Biden, other Democratic and Republican politicians in the US, and the Hong Kong pro-democracy movement.

At the very end of March of this year, this operation created a handful of fake accounts that posted for a few weeks at a low volume — typically around a dozen posts each in total, with most accounts falling silent in mid-April. One posted comments in Chinese, and criticized the United States and the Hong Kong pro-democracy movement. Other accounts posed as conservative Americans and posted memes in English that accused President Biden and other politicians — both Democrats and Republicans, including House Speaker Nancy Pelosi, Climate Envoy John Kerry and Senator Mitt Romney — of corruption; called for protecting gun rights and restricting abortion access;

praised politicians who supported those policies; and accused the US government of running bioweapons labs in Ukraine. One other account in this cluster posted similar accusations, but in French.



Image

Pro-life comment posted by an account in *cluster number two* in reply to a news article about Florida Governor Ron DeSantis, April 14, 2022.

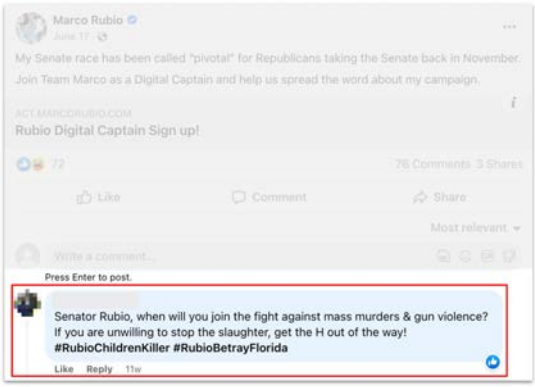
CLUSTER NUMBER THREE

Key takeaways:

- Poste from April to August 2022
- Posted primarily in English
- Fake accounts posed as liberals in Florida, Texas and California
- Themes: pro-choice and pro-gun reform in the US, criticism of Republican party and Sen. Rubio (FL)

Starting at the end of April of 2022, a handful of accounts and Pages posted sporadically into early August, at which point most of them fell silent. They posed as liberal Americans living in Florida, Texas and California and posted criticism of the Republican Party for its stance on abortion access and gun rights. Other posts focused on individual politicians, particularly Senator Rubio, but also Senators Rick Scott and Ted Cruz, and Governor Ron DeSantis. They were joined by one account from *cluster number two* which "flipped" from anti-Biden posts to pro-abortion-rights content. This third cluster was active longer than others.

One account that the operation added in June impersonated a student activist in California, including using their photos of a student protest. However, it did not post any further, and had no likes, shares or friends by the time we took it down.



Image

Comment by an operation account in reply to a post by Senator Rubio.

CLUSTER NUMBER FOUR

Key takeaways:

- Posted from July to September 2022
- Posted in Czech
- Fake accounts posed as Czechs
- Themes: domestic politics in Czechia, energy prices and inflation, criticism of the Czech government and its support of Ukraine at the expense of the Czech people, and the government's policy toward China.

At the end of July, the operation set up one Group and a handful of accounts that posed as people in the Czech Republic and posted in Czech a few times a day. They shared memes and text posts that criticized the Czech government. Some posts focused on domestic issues, including high energy prices and inflation as a result of supporting Ukraine. Others accused the Czech government of prioritizing Ukraine over its own citizens and being a "puppet" of the EU or US. A few criticized the government's approach to China and warned against antagonizing it. "A trade war with China will hurt more than with Russia," one post said.

Image

Group created by *cluster number four*

Translation

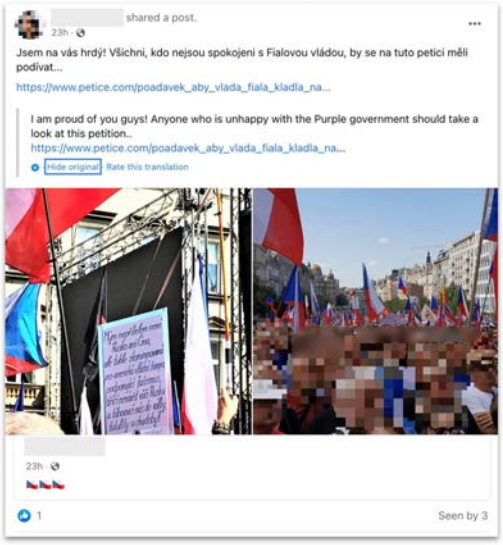
Group name: "Return the Czech Republic to the Czechs!"

Group's *About* section: Citizens must be at the center of attention of the Czech government.

In this group, you can freely express your dissatisfaction and anger with Fiala's rule, not only in domestic matters, but also in foreign policy. Discuss how to take legitimate actions to force the Purple Government to change, or even overthrow it!

This Czech-focused effort included a broader range of activity, including off-platform. For example, one post asked people to write anti-government messages offline, photograph them and email the pictures to the operator. The appeal noted, "Our goal is to get rid of the current government, which just wants to be the star of Europe, and create a government that will actually care about the interests of Czech citizens".

They also created an anti-government petition, which they ran on two different Czech petition sites in late July and early August. The petition touched on a range of issues, including a call not to antagonize Russia and China, concluding: "It is also important to prevent China's abandonment of the 16+1 initiative from triggering economic retaliation from China, as we cannot afford the wrath of two great powers at the same time".

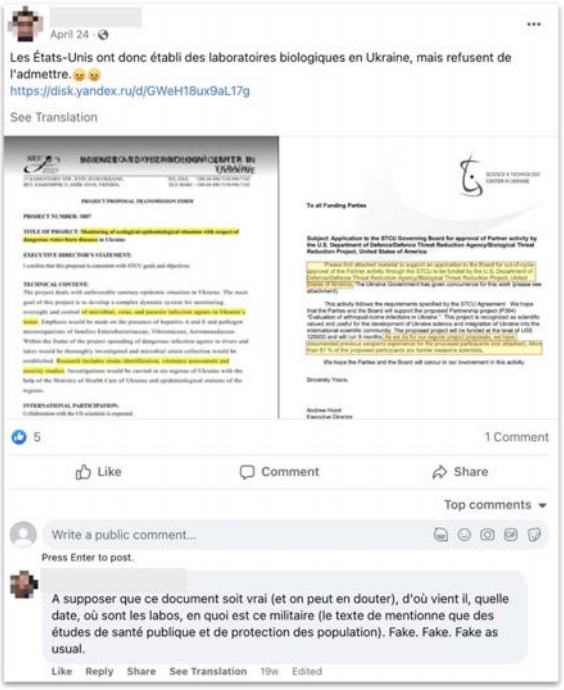


Image

Post by one of the operation's Czech accounts, sharing a post by another of the operation's accounts, together with a link to a petition created by the operation.

RUSSIA-CHINA: NARRATIVE OVERLAP

On a number of occasions, this Chinese-origin operation shared content posted by various Russian state-linked entities. For example, on April 24, the French-language account from *cluster number two* posted a link to an alleged cache of documents claiming that the US had run bioweapons projects in Ukraine. Only one unconnected user replied to the post, calling it out as a fake. That link had originally been published by the Russian Ministry of Defense, including on Telegram on April 14, ten days prior to it being re-shared by the Chinese network.



Image

Post by the French-language fake account sharing allegedly "leaked" documents.

Translation

Post: So the United States set up biological labs in Ukraine, but refuse to admit it.

[link]

Comment by an authentic, unconnected user: Supposing this document is real (which is doubtful), where is it from, what date, where are the labs, and what's military about it (the text only mentions public-health studies and protecting the population). Fake. Fake. Fake as usual.

On another occasion, a Czech account from *cluster number four* posted a link to a translation of an RT article about US global interference, with the text, "What good is this escalation for average Americans? Czechs? Fortunately, China is more rational, otherwise World War III would break out."

Image

Post by the operation, showing the link to the Czech article. All three reactions to this post were from operation accounts.

02

Russia

EXECUTIVE SUMMARY:

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

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

This is the largest and most complex Russian-origin operation that we've disrupted since the beginning of the war in Ukraine. It presented an unusual combination of sophistication and brute force. The spoofed websites and the use of many languages demanded both technical and linguistic investment. The amplification on social media, on the other hand, relied primarily on crude ads and fake accounts. In fact, on our platforms, the majority of the accounts, Pages and ads were detected and removed by our automated systems before we even began our investigation. Together, these two approaches worked as an attempted smash-and-grab against the information environment, rather than a serious effort to occupy it long-term.

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

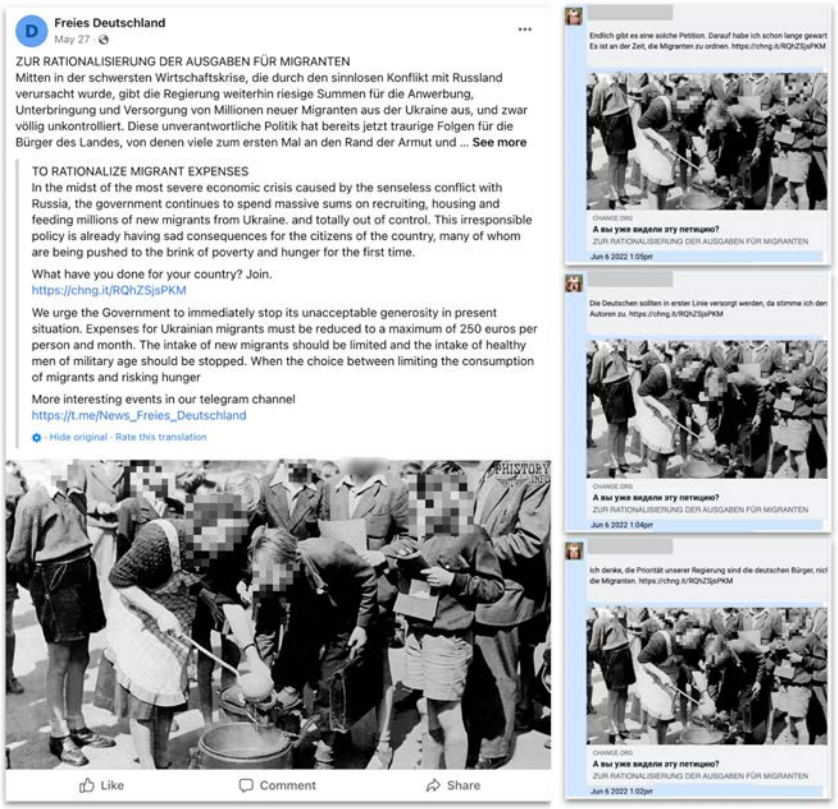
TAKEDOWN BY THE NUMBERS

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

WARMING UP WITH ITS OWN ECHO CHAMBER

From the start, the operation built mini-brands across the internet, using them to post, re-share and like anti-Ukraine content in different languages. They would create same-name accounts on different platforms that served as backstops for one another to make them appear more legitimate and to amplify each other. It worked as a fake engagement carousel, with multiple layers of fake entities boosting each other, creating their own echo chamber. Many of these accounts would get routinely detected and taken down for inauthenticity on our platform.

On May 27, the operation ran a German-language petition on change[.]org, demanding that the German government stop its “unacceptable generosity” toward Ukrainian refugees. This petition promoted a Telegram channel called “News Freies Deutschland” (News Free Germany) and was signed by an account on change[.]org called “Freies Deutschland” (Free Germany). Then, a Facebook Page with no followers run by the operation under the same name (created on May 15) promoted the petition and this Telegram channel. On Facebook, a number of fake accounts began sharing the link to the petition, Telegram channel and Facebook Page, while also promoting each other. In the end, the vast majority of the shares of these links on Facebook came from the operation’s own accounts.



Image

Left: post by the "Freies Deutschland" Page on May 27, promoting the petition and "our" Telegram channel.

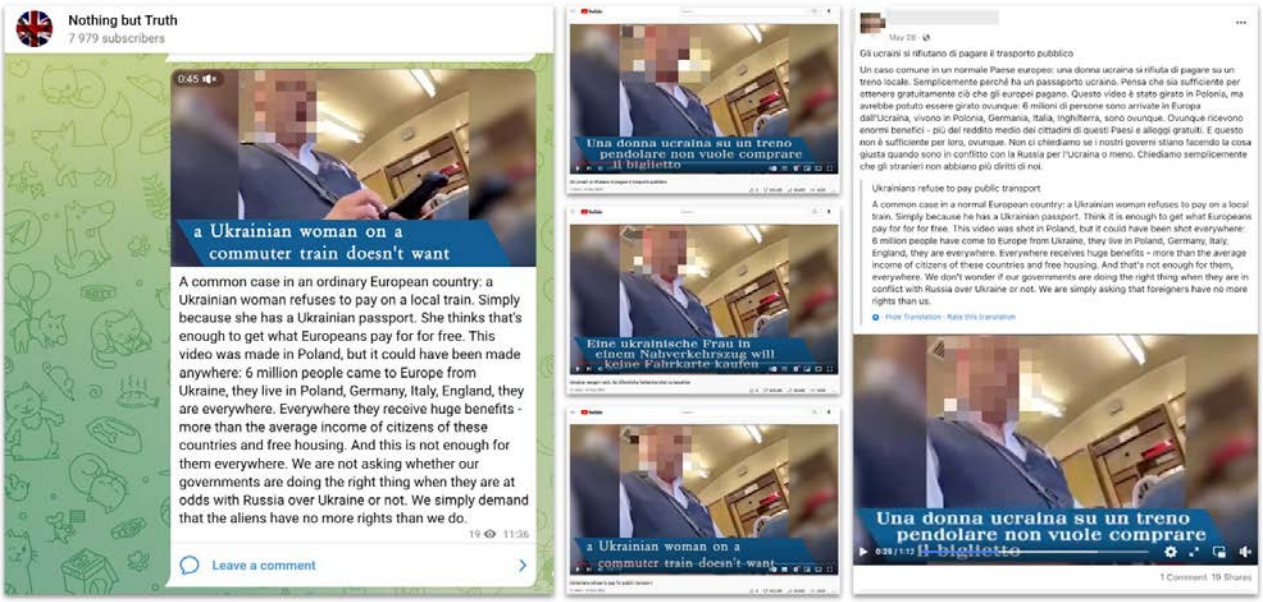
Right: three comments from a fake account sharing the petition, posted within five minutes of each other on June 6 in reply to posts by German news outlets Deutschland.de, Der Spiegel and Tagesschau.

Translation: comment #1: At last there's a petition like this. I've been waiting for it for a long time. It's time to get the migrants in order.

Translation: comment #2: Germans should be cared for first, I agree with the authors.

Translation: comment #3: I think German citizens are our government's priority, not the migrants.

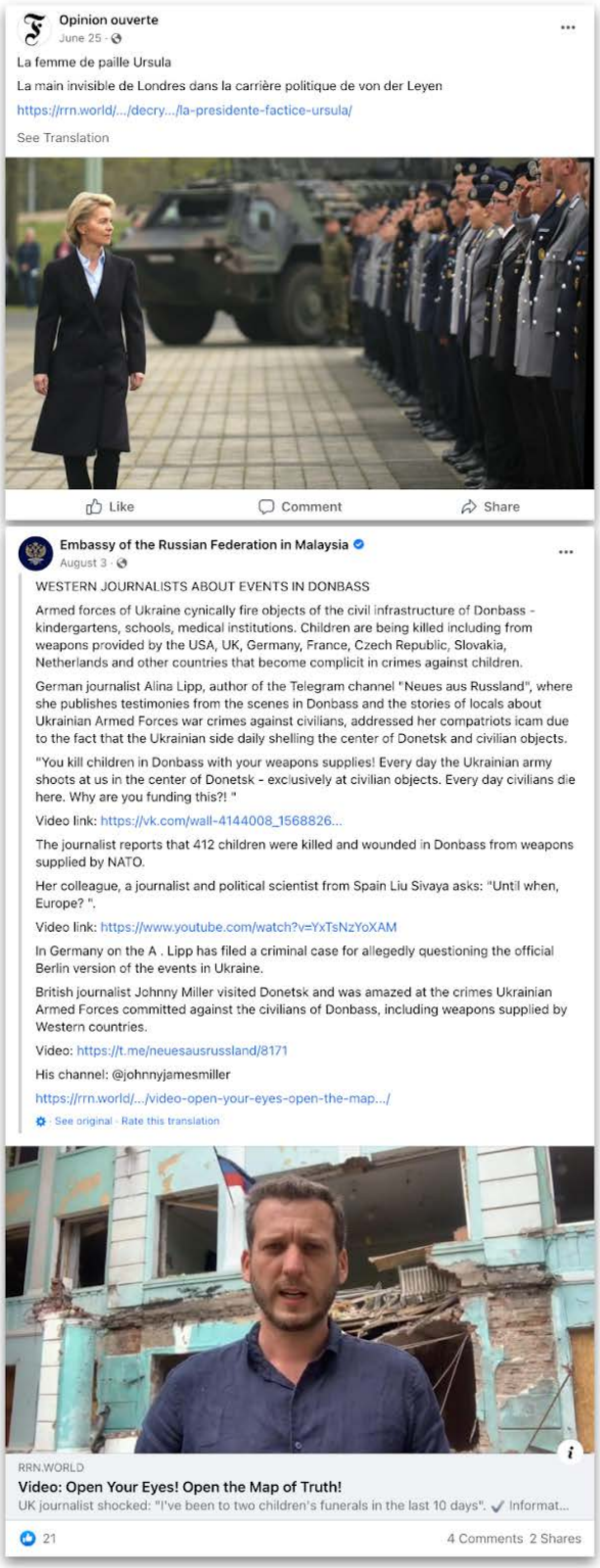
This early phase of the operation also made use of videos. In one case, we saw a number of YouTube and Telegram channels posting the same videos about rising prices in Europe caused by sanctions on Russia, and accusing Ukrainian migrants of theft, vandalism, prostitution, violence and not paying for train tickets. Interestingly, while the video footage was identical, different channels featured subtitles in different languages — German, English and Italian.



Image

Three versions of the same video on Telegram (left), YouTube (center), and Facebook (right). The Telegram post was made on May 27. The Facebook posts were made on May 28 within two hours of each other. The YouTube videos on May 30 within 40 minutes of each other.

Early on, the people behind this activity also made some efforts to create multi-platform, multi-language media brands of their own. On June 6, 2022, they created a brand called RRN, or Reliable Recent News, hosted at rrn[.]world. This website operated in multiple languages: English, French, German, Spanish, Italian, Chinese and Arabic. It posted lengthy articles and graphics. While it did not run branded accounts on Facebook or Instagram, it appeared to maintain accounts on Twitter and Telegram, which were amplified by the operation's Facebook Pages. The Facebook Pages of the Russian diplomatic missions in Malaysia, Sweden, Hungary, Slovakia and Bangladesh shared links to the site.



Image

Links to rrn[.]world posted by one of the operation's fake accounts (top) and the Russian Embassy in Malaysia (bottom).

Translation of the top post:

Ursula, the straw woman.

The invisible hand of London in von der Leyen's career.

The operation also ran other brands that were smaller and not as well-developed. Typically, they consisted of a Facebook account and Page, Telegram channel, and one or more other social media

channels, including YouTube, Instagram or Twitter, and other, less-mainstream forums. For example, they ran a brand “The truth is not a weapon” with at least one Telegram channel, one Facebook Page and three YouTube channels, translated into English, German and Italian.

Notably, the operation did not run all the elements of these mini-brands at the same time. Instead, they appeared to have experimented with different formats and channels over time. For example, one posted long articles on Telegram and LiveJournal in May, then in June switched to memes and shorter articles on Facebook. Another brand, called “Nothing But Truth,” posted videos on YouTube in May, then switched to sharing memes and short text posts on Facebook in June. We saw most of these brands switch in this manner around the same time — in late May and early June — for unknown reasons.

Image

Left, YouTube video by “Nothing But Truth”, June 10, the last video this channel posted.

Right, meme by the same brand on Facebook, June 13.

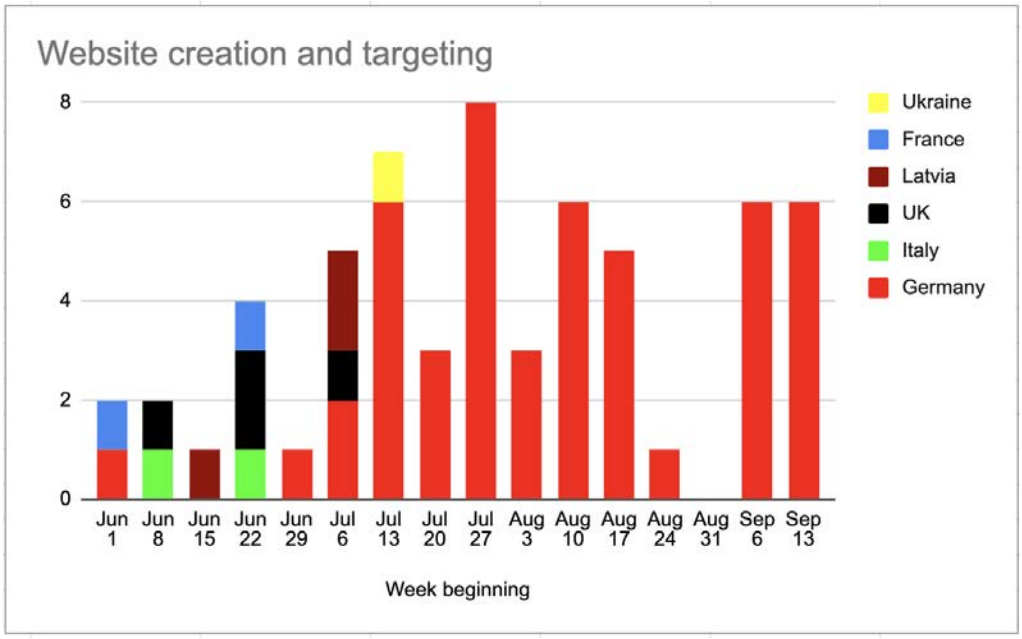
BUILDING WEB INFRASTRUCTURE TO IMPERSONATE MEDIA

In early June, the operation shifted tactics. Between June 9 and mid-September, it created more than 60 websites that mimicked the exact layout and spoofed web addresses of mainstream European media outlets like Der Spiegel, the Guardian and Italian news agency ANSA. These fake websites hosted videos and articles that portrayed the Ukrainian government and armed forces as criminal and corrupt, Russia as the victim of Western aggression, and Western sanctions as perilous for Europe and its citizens.

Initially, the balance between targeted countries was largely even; between June 5 and July 14, the operation set up more than 15 websites that impersonated legitimate news sites. One of them focused on Ukraine, two on France, two on Italy, three on Latvia, four on the UK and five on Germany.

Starting July 16, the balance changed. The operation created at least 40 more domains that spoofed German news sites, and no other countries at all. Some of these were new top-level domains for news organizations it had already impersonated in June. For example, the domain bild[.]pics was created on June 5 and bild[.]llc on July 25, both impersonating Bild Zeitung.

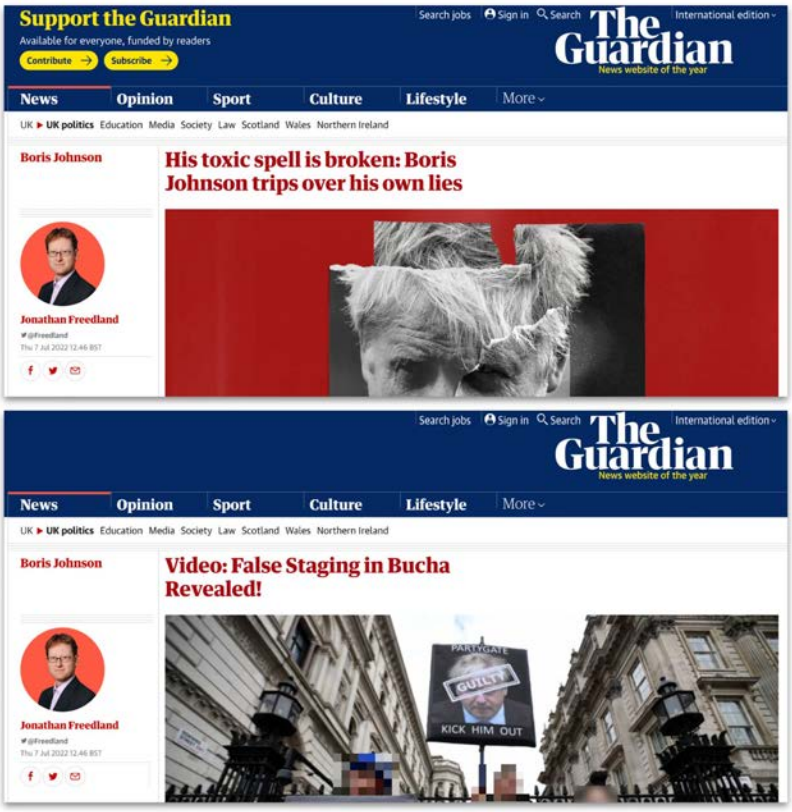
The website creation slowed in late August, then accelerated once more in September after we began blocking the operation's domains as we identified them.



Image

The operation's creation of websites, June-September 2022, broken down by country.

The fake websites appeared to have been built with particular care. They would copy the appearance of the target news site, interspersed with links to that real site and even used its cookie acceptance page. In some cases, they went even further. For example, in early July, the website mimicking The Guardian posted an article that accused Ukraine of staging the murder of civilians during the Russian occupation of Bucha. The spoofed version used the photo of a real Guardian journalist and the same timestamp as an authentic Guardian article by that journalist, published on the same day that the fake news site was registered. The spoofed version also embedded working links to the genuine Guardian's live-news ticker and news front page. The mimicry was not perfect — the spoof omitted the original's "Support the Guardian" banner, and not all its links worked — but it showed investment into making the site appear authentic so it could withstand at least some casual scrutiny. This tradecraft is remarkably similar to that of the Iranian operation known as "Endless Mayfly," exposed by Citizen Lab in 2019.



Top image

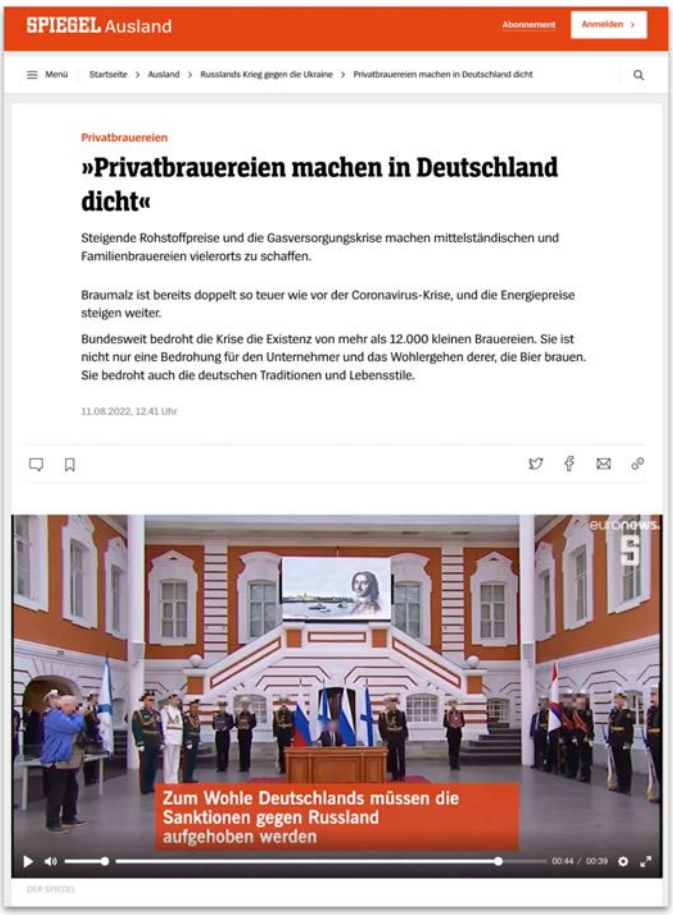
Screenshot of an article on the genuine Guardian website theguardian[.]com, July 7, 2022, showing the author and timestamp on the left.

Bottom image

Screenshot of an article on the spoofed Guardian website theguardian[.]co[.]com, showing the same author and timestamp, but a different text and photo. The website was registered that day.

The operation coordinated publishing across multiple languages. For example, the same article about Bucha was published on the same day in English on the spoofed Guardian site, in Italian on the spoofed ANSA site, and in German on the spoofed Spiegel site. It also appeared in English, French, German, Italian, Spanish and Chinese on rrn[.]world.

While some articles focused on war and geopolitics, others approached issues more indirectly, focusing on general social or economic problems before linking those to EU sanctions against Russia for its invasion of Ukraine.



Image

Screenshot from an archived version of an article posted by the operation on the website spiegelr[.]live, spoofing the genuine Der Spiegel site. The article focused on the plight of German breweries because of rising energy and grain prices. Only at the end of the video did the caption read, "For the good of Germany, the sanctions against Russia must be lifted."

CRUDE AMPLIFICATION

While the spoofed websites and articles were built with some care, the operation took a brute-force approach to amplifying them on social media. Its approach appears to have been to run a large number of basic ad and crude fake accounts, in the hope that at least some would remain undetected by platforms and researchers long enough to reach target audiences. In fact, on Facebook, our automated systems detected and disabled the majority of these accounts, posts and ads, and investigative journalists and open-source researchers identified some of the spoofed websites. This was a resource-intensive and noisy approach that resulted in a very high number of disabled assets.

Much of the amplification was done by fake accounts that made only the most limited efforts to appear convincing. Many were created in batches and had profile pictures likely generated using artificial intelligence techniques like generative adversarial networks (GAN). An unusually large number of these fake personas claimed to work at Netflix. The operation also ran a large number of ad accounts to promote its Pages and posts. Like their Facebook accounts, many were disabled by our automated systems before or soon after they started running ads.

Even the operation's Pages tended to be crudely made and repetitive, as if they had been set up in batches, and never given more of an attempt at a distinct identity. Many used a stylized Gothic "F" as their logo, like that of German newspaper the Frankfurter Allgemeine Zeitung (FAZ), but they made no attempt to resemble the FAZ in other ways. Many had names that followed a standard pattern: an adjective or adverb, two or three letters and a number, like "Physically zjc3" or "Splendid lc8." Dozens more had names that meant "open opinion" in German, French or Italian (Offene Meinung, Opinion Ouverte, Opinione Aperta). Still, others used the name of one German media outlet, but the logo of another — for example, the name WAZ (for Westdeutsche allgemeine Zeitung) with the logo of T-Online.

Top image

Share of the spoofed Guardian link by one of the operation's Pages on July 11: note the Gothic "F" for its profile picture.

Bottom image

Share of a link to the German version of the Bucha story on a spoofed Spiegel website by another of the operation's Pages, named "Public Opinion," July 15. The meme reads, "End the game with Ukraine."

The main activity of all these assets was amplifying the operation's off-platform content, rather than creating anything new on-platform. The Pages typically shared links to the spoofed web articles, sometimes with accompanying memes or graphics. The fake accounts posted the links as comments on authentic Pages in the target country. Sometimes, accounts would change their language from one week to the next. Typically, one account would post the same link up to a dozen times, with a different comment each. Public reporting has described thousands of posts on Twitter from accounts that behaved similarly.

The operation did appear to pay some attention to its audience. When its accounts commented on other people's Pages, they often chose verified Pages with high follower counts. This was likely to leverage the verified Pages' audiences and increase the operation's own chance of reaching an audience. Very often, the choice of Pages was appropriate to the subject matter: for example, comments in reply to news reports about the war or energy prices. However, other comments were under Pages that had nothing to do with the war in Ukraine, or even with politics. These included comments on sports, fashion and even a post by Playboy Germany.

Image

A post by the verified Page of WWE Deutschland, together with the reply by one of the operation's fake accounts.

Translation:

Post: Good morning.

Comment: The only weapon that my country should deliver to Ukraine.

This on-platform amplification did not come close to the sophistication of the website spoofing aspect of this operation. Instead, it resembled an attempt to push the fake domains as widely as possible as fast as possible, in the hope that at least some real people might see the fake websites before they were exposed. It was a resource-intensive and noisy approach with a high degree of

automated disables and the overwhelming majority of shares of the spoofed domains on our services coming from the operation itself.

Appendix: Threat indicators

1. CHINA

We assess that the following petitions were created by this operation. Open-source research may use these as leads to look for additional activity across the internet, but it's important to note that the mere sharing of these links would be insufficient to attribute any account to the operation without corroborating evidence because they might also be shared by real people.

- https://www.petice[.]com/poadavek_aby_vlada_fiala_kladla_na_prvni_misto_zajmy_svych_oban
- https://e-petice[.]cz/petitions/pozadavek-aby-vlada-fiala-kladla-na-prvni-misto-zajmy-svych-obcanu-1.html

2. RUSSIA

Domains

Please note that the individuals behind this activity continued to create new domains over time and in response to our enforcement. Given the sprawling and persistent nature of the operation, this list should not be taken as exhaustive and might present an important area of research for the open-source community to help expand our collective understanding of this operation's web infrastructure.

Domain	Registration date	Country
Avisindependent[.]eu	6/3/2022	France
bild[.]pics	6/6/2022	Germany
rrn[.]world	6/6/2022	Multiple
dailymail[.]top	6/10/2022	UK
repubblica[.]life	6/13/2022	Italy
delfi[.]life	6/15/2022	Latvia
dailymail[.]cam	6/23/2022	UK
dailymail[.]cfd	6/23/2022	UK
20minuts[.]com	6/28/2022	France
ansa[.]ltd	6/28/2022	Italy
spiegel[.]ltd	6/29/2022	Germany
theguardian[.]co[.]com	7/7/2022	UK

bild[.]asia	7/12/2022	Germany
bild[.]vip	7/12/2022	Germany
delfi[.]today	7/12/2022	Latvia
delfi[.]top	7/12/2022	Latvia
rbk[.]today	7/13/2022	Ukraine
spiegel[.]today	7/16/2022	Germany
spiegel.fun	7/18/2022	Germany
spiegel.quest	7/18/2022	Germany
tonline[.]cfd	7/18/2022	Germany
tonline[.]life	7/18/2022	Germany
tonline[.]today	7/18/2022	Germany
spiegel[.]pro	7/20/2022	Germany
bild[.]eu[.]com	7/24/2022	Germany
bild[.]llc	7/25/2022	Germany
spiegeli[.]life	7/28/2022	Germany
spiegeli[.]live	7/28/2022	Germany
spiegeli[.]today	7/28/2022	Germany

welt[.]ltd	7/28/2022	Germany
faz[.]ltd	7/30/2022	Germany
t-onlinr[.]life	7/31/2022	Germany
t-onlinr[.]live	7/31/2022	Germany
t-onlinr[.]today	7/31/2022	Germany
spiegel[.]agency	8/6/2022	Germany
schlauespiel[.]de	8/9/2022	Germany
tagesspiegel[.]ltd	8/9/2022	Germany
spiegelr[.]live	8/14/2022	Germany
spiegelr[.]today	8/14/2022	Germany
t-onlinl[.]life	8/14/2022	Germany
t-onlinl[.]live	8/14/2022	Germany
t-onlinl[.]today	8/14/2022	Germany
sueddeutsche[.]me	8/18/2022	Germany
spiegel[.]ink	8/20/2022	Germany
sueddeutsche[.]online	8/20/2022	Germany
t-online[.]life	8/20/2022	Germany

nd-aktuell[.]net	8/23/2022	Germany
zestiftung[.]com	8/27/2022	Germany
bild[.]ws	9/12/2022	Germany
faz[.]agency	9/12/2022	Germany
nd-aktuell[.]pro	9/12/2022	Germany
spiegel[.]work	9/12/2022	Germany
sueddeutsche[.]cc	9/12/2022	Germany
welt[.]ws	9/12/2022	Germany
sueddeutsche[.]co	9/13/2022	Germany
tagesspiegel[.]co	9/13/2022	Germany
welt[.]media	9/13/2022	Germany
bild[.]work	9/14/2022	Germany
spiegel[.]cab	9/14/2022	Germany
fraiesvolk[.]com	9/17/2022	Germany

Telegram channels, petitions and blogs

- https://t[.]me/news_munchen/42
- https://t[.]me/News_Freies_Deutschland
- https://t[.]me/friekorps
- https://t[.]me/ex_pat

- https://t[.]me/berlin_noname
- https://t[.]me/meun_01
- https://t.]me/milano_vs
- https://t.]me/via_napoli
- https://t[.]me/Streetleeds
- https://t[.]me/london_rumors
- https://t[.]me/birmingemS
- https://t[.]me/london0101
- https://t[.]me/reliablerecentnews
- https://marc-foreman[.]livejournal[.]com/
- https://chng[.]it/NYt5whb9Nr
- https://chng[.]it/shjPpqH2Cg
- https://chng[.]it/dm7xNLS22d
- https://chng[.]it/RQhZSjsPKM
- https://chng[.]it/HWDDBjGpxF
- https://www.change[.]org/p/zur-rationalisierung-der-ausgaben-f%C3%BCr-migranten
- https://www.change[.]org/p/f%C3%BCr-unvoreingenommene-berichterstattung-%C3%BCber-den-krieg-in-der-ukraine
- https://www.change[.]org/p/zur-bew%C3%A4ltigung-der-folgen-der-wirtschaftskrise
- https://www.change[.]org/p/tighten-legislation-regarding-migrants
- https://www.change[.]org/p/no-weapons-to-ukraine