

Verified Disinformation:

How X Profits From the Rise of a Pro-Kremlin Network

About the Authors and Organization

Aleksandra Atanasova, Riccardo Giannardi, Pelin Ünsal

Reset Tech is a fully independent global enterprise with not-for-profit operations in North America, Europe, and Australia. Our mission is to guard against digital threats to our security, safety, and fundamental rights. We seek to "reset" the connection between media and democracy and restore the promise of technology that works for people and free expression.

For more information, visit reset.tech.

Copyright © 2024 Reset Tech. All rights reserved.

Executive Summary

This report identifies a rapidly expanding network of inauthentic accounts on **X**, which has doubled in size and activity over five months. The network disseminates Kremlin-aligned propaganda in six languages, using paid verification to amplify its reach.

We monitored this network for five months, ascribing it to a distinct branch of Russia's ongoing Doppelganger operation. The network is part of a broader ecosystem of 6,500 accounts—mostly dormant assets—used in earlier campaign phases to target audiences in the EU and beyond with pro-Kremlin propaganda. All accounts in this network display clear markers of coordinated inauthentic behavior (CIB).

First identified in June 2024 as clusters of accounts sharing content in five languages: French, German, English, Russian, and Turkish, the network has since doubled in size to 530 accounts and added Polish as a sixth language. Between June and October 2024, it generated at least 16,000 posts.

The campaign strategically exploits two platform-specific features to boost content visibility: X's trending hashtags and blue verification checkmarks. The latter also provides direct financial benefit for X, as the blue checkmark is a paid feature on the platform. Using verified accounts to enhance perceived legitimacy and amplify content has been a central tactic in another campaign on X recently investigated by Reset Tech. Our findings show that this feature is increasingly popular among disinformation and scam campaigns on the platform.

The campaign poses a risk to electoral processes by promoting narratives that align with Russia's political agenda. Notably, 40 percent of all posts across different languages spread propaganda about Ukraine. Like other Kremlinaligned operations like Doppelganger and Overload, this campaign references reputable media outlets to enhance the credibility of its propaganda. However, unlike Doppelganger, the accounts in this network do not share links to external domains that mimic Western media websites. Instead, they keep the content within the platform, using various media formats. The campaign primarily utilizes Al-generated videos that feature multilingual captions and voiceovers.

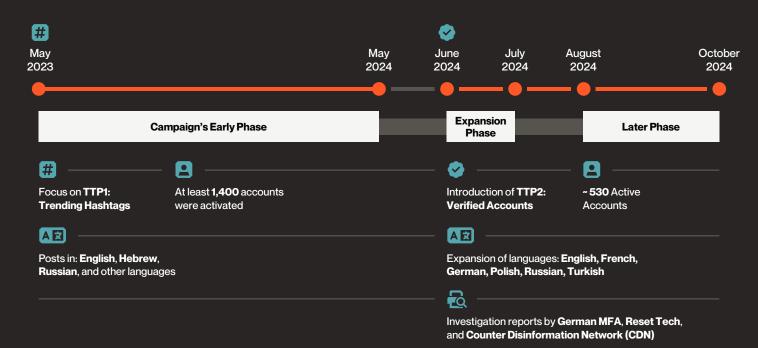
Despite evident coordination, X has not yet suspended the entire network. As of October 31, 36 percent of the 530 analyzed accounts remain active, while the broader ecosystem of dormant accounts remains largely intact.

Contents

Introduction	6
The Content Strategy	8
Focus on Ukraine	8
Narratives Across Languages	9
Media Formats and Content Analysis	11
Amplification Tactics	14
Blue Checkmarks and Trending Hashtags	14
The Network: Coordinated Activity in Clusters	15
Coordinated Posting	15
Accounts Clusters	17
The Broader Ecosystem: Dormant Accounts from Earlier Phases	21
Insufficient Response to the Campaign by X	25
Conclusion	26
Disclaimer	26

Investigation Timeline

This timeline shows how key phases of the investigated network's disinformation campaign evolved from May 2023 to October 2024, with shifts in account activity, language use, and tactics.





Introduction

Coordinated networks of inauthentic accounts continue to spread political content and pro-Kremlin disinformation on X, with limited oversight from the platform. Since early 2024, Reset Tech has been monitoring the activities of a specific campaign, attributing it to a distinct branch of the Doppelganger operation.

We initially reported on this campaign in July 2024, identifying two key tactics used by its operators: leveraging verified accounts to disseminate content directly within X-avoiding external links-and exploiting trending hashtags to increase visibility to targeted audiences. While the Doppelganger operation is primarily known for using accounts to share links to domains that impersonate legitimate news sites, we attributed this campaign to Doppelganger due to the notable content similarities, references to reputable media outlets, and overlapping narratives. Both campaigns clearly align with the Kremlin's political agenda, sharing objectives such as tarnishing Ukraine's reputation, discouraging Western support for Ukraine, sowing division between EU allies, and fostering support for Russia.

Unlike Doppelganger, the content distributed in this campaign is specifically designed for direct consumption within the platform, videos being the preferred content type. In this way, the actors align their dissemination strategy with that of another pro-Kremlin Foreign Information Manipulation and Interference (FIMI) campaign, Operation Overload, investigated by Reset Tech and the Finnish company CheckFirst in June 2024. Like Overload, the content shared on X is confined to the platform and places a strong emphasis on video. However, from a content standpoint, the analyzed campaign differs significantly from Overload. Unlike Overload, the campaign's activities on X are multilingual, targeting a broader audience instead of just the research community. Thus, the operators align more closely with Doppelganger's objective of flooding online information spaces with pro-Kremlin content in multiple languages.

Referring to reputable media outlets to boost the credibility of Kremlin propaganda appears to be a common tactic in pro-Russian operations. Doppelganger employs cloned media domains for this, while campaigns like Overload and the one examined in this report reference established Western outlets as sources, either in the copy of the social media posts or through logos embedded in various media formats.

Recently, several reports have explored the Doppelganger operation on X, albeit with a cursory focus on this specific campaign. For instance, in June 2024, the German Ministry of Foreign Affairs released an extensive report on Doppelganger's activities on X, noting that content is also being shared without links. In September 2024, Alliance4Europe/CeMAS and researchers from the Counter Disinformation Network (CDN) also published a report on the operation on X, highlighting several posts that did not include any associated URLs.

This report provides a comprehensive overview of the campaign over the past five months. It emphasizes the consistent tactics used and examines how the platform has responded to the coordinated behavior of an etwork of inauthentic accounts. Additionally, we expanded our research to map a larger network of dormant X accounts that could be reactivated at any time. Since the release of our first report in July 2024, the network has continued to generate content related to the campaign at double the capacity. We identified 530 inauthentic anonymous accounts between June and October 2024. This network generated at least 16,000 posts during that period.

Polish has also been added to the list of languages used in the operation, alongside English, German, French, Russian, and Turkish. The content in six languages is tailored for specific audiences and strategically designed to leverage local topics that resonate with target markets while promoting pro-Kremlin disinformation. Although X has removed many accounts, a significant part of the network—36 percent—remains active as of October 31, 2024. New accounts are continuously being created to sustain this activity.

The operator's recurring tactic, technique, and procedure (TTP) involves using verified X accounts to distribute content. This strategy is designed to increase the organic reach of posts on the platform. We have observed this tactic in another recent campaign we monitored on X, targeting audiences with scam content related to dubious financial investments. Typically, the inauthentic accounts obtain a paid blue checkmark from X before posting content, which helps enhance their visibility and credibility.

Even when the accounts do not run paid advertisements, X directly benefits from such campaigns. The second TTP used in the campaign involves leveraging trending hashtags to reach target audiences. The accounts alternate between different combinations of hashtags, reposting the same content multiple times with various hashtags to increase visibility.

The report also focuses on different clusters of accounts involved in the campaign, highlighting distinct indicators of CIB. These include synchronized activation, aligned posting histories, identical timelines, and common branding and bio details. We identified three distinct categories of accounts, each with unique characteristics. Notably, we observed coordinated posting of content related to NFTs and cryptocurrencies before and after the accounts' participation in the campaign. This suggests that some of these assets are being utilized for other initiatives on X as a revenue-generating strategy.

Lastly, we explore a broader ecosystem of inauthentic accounts on the platform. We identified a coordinated network of at least 6,500 latent **X** accounts that exhibit similar posting behaviors to some of those analyzed in our study. Many of these accounts are either inactive or have been repurposed for other activities.

By mapping identical posts, we identified connections to other X accounts in the Doppelganger operation earlier in 2024. These accounts shared content in multiple languages, including Hebrew, Ukrainian, and Italian. We chose not to examine the earlier phases of the campaign, as those accounts operated slightly differently—they generated fewer posts before becoming inactive. They did not use verified accounts for content dissemination.

Nonetheless, we can confirm that between May 2023 and May 2024, 1,400 accounts published similar content using trending hashtags on X to target various audiences. Notably, these accounts remain active on the platform today as dormant assets that can be easily repurposed to create new content at any time. Our findings raise concerns about the effectiveness of X's measures to address coordinated activities by inauthentic networks on the platform.

The Content Strategy

The current phase of the campaign began in early June 2024 and involves a network of verified and non-verified X accounts. These accounts are typically activated in mixed clusters, consisting of between five and thirteen accounts organized by language, and used to post content simultaneously in specific languages. Each account posts two to three tweets daily. In quick succession, all accounts in an active cluster share the same content with slight text variations, accompanied by identical media. While some accounts have maintained consistent posting throughout the analyzed period, others typically share between 15 and 30 posts before becoming inactive or getting suspended. As a result, new accounts are introduced into the campaign every few weeks to replace those that have become inactive. Throughout the analyzed period from June to October 2024, we observed systematic, coordinated activity in six languages: English, French, German, Russian, Turkish, and Polish. Notably, Polish was introduced last, with activity beginning in late June.

Focus on Ukraine

The campaign covers a variety of topics across different languages, sometimes significantly. However, most of the content tends to reinforce typical pro-Kremlin narratives. Posts related to Ukraine account for over 40 percent of all content. Below is a list of the most common narratives we observed across the six languages:

Delegitimizing Ukraine's government:

Claiming that Ukraine is destined to lose the war; the country is plagued by corruption, its army is demoralized and weak, and Western countries will eventually halt their weapon deliveries. Questioning the legitimacy and functionality of Ukraine's government, often framing it as corrupt or ineffective.

Opposing Western support for Ukraine:

Criticizing Western countries' financial and military support for Ukraine; often framing it as wasteful or harmful to local economies.

Portraying NATO as aggressive:

Depicting NATO as a threat to stability; suggesting its actions provoke conflict and jeopardize international security.

Emphasizing Russian strength and stability:

Promoting Russia's resilience and self-sufficiency. Portraying the country as a stabilizing global force.

Highlighting divisions within the West:

Amplifying social and political conflicts within Western countries; implying weakening alliances and internal instability. Seeking to pit the U.S. against Europe regarding the war and suggesting that Europe will ultimately bear the financial burden.

Narratives Across Languages

In addition to Ukraine-focused narratives, several posts leverage current events, reshaping them to align with the Kremlin's agenda. The campaign's top targets are the U.S. elections, NATO, the EU, the U.S., and European political leaders such as U.S. President Joe Biden, U.S. Vice President Kamala Harris, French President Emmanuel Macron, and German Chancellor Olaf Scholz.

Numerous posts in all the mentioned languages, particularly English, focus on the U.S. elections. They portray Biden as ineffective and criticize Harris after her announcement as a Democratic candidate. These posts also leverage the U.S. elections to raise skepticism about the future of U.S. military support for Ukraine.

The network exploits current events in specific countries to heighten criticism of national leaders. The French cluster shows significant backlash against Macron over his immigration policies and support for Ukraine, with some posts emphasizing his dwindling popularity. Similarly, in the German cluster, Scholz is criticized for allegedly excessive financial aid to Ukraine, raising questions about his integrity. His lack of action in response to the economic crisis in Germany and his support for migrants are also criticized. The network similarly questions the positions of France and Germany regarding the Israel-Hamas war. The French Olympics are also targeted with narratives aiming to undermine France's position on the global stage.

Turkish narratives highlight the struggles of the local economy, noting that Turkish companies face difficulties due to U.S. sanctions against Russia, resulting in bankruptcies and widespread unemployment. Additionally, some posts indicate that U.S. economic demands have intensified social divisions within Turkey and suggest President Reycepp Erdoğan, disillusioned with the EU, is redirecting Turkey's attention toward BRICS.

Polish narratives center on the Ukraine-Russia conflict, highlighting the pressure placed on the Polish economy. Criticism of support for Ukraine and questions of NATO's effectiveness are also prominent. In particular, Polish accounts emphasize that EU policies and dependence on the U.S. are damaging the domestic economy, suggesting a need for a stronger coalition and attempting to shift focus toward a partnership with Russia.

Russian posts center solely on Ukraine's deteriorating position, both economically and due to the ongoing war. They feature bleak portrayals of mobilization efforts, economic collapse, and critiques of Ukrainian government officials and President Volodymyr Zelenskyy while simultaneously portraying Russia as the ultimate winner.

The Network Addresses Current Events in Local Languages

Number of posts by accounts of the network between June and October 2024, by language

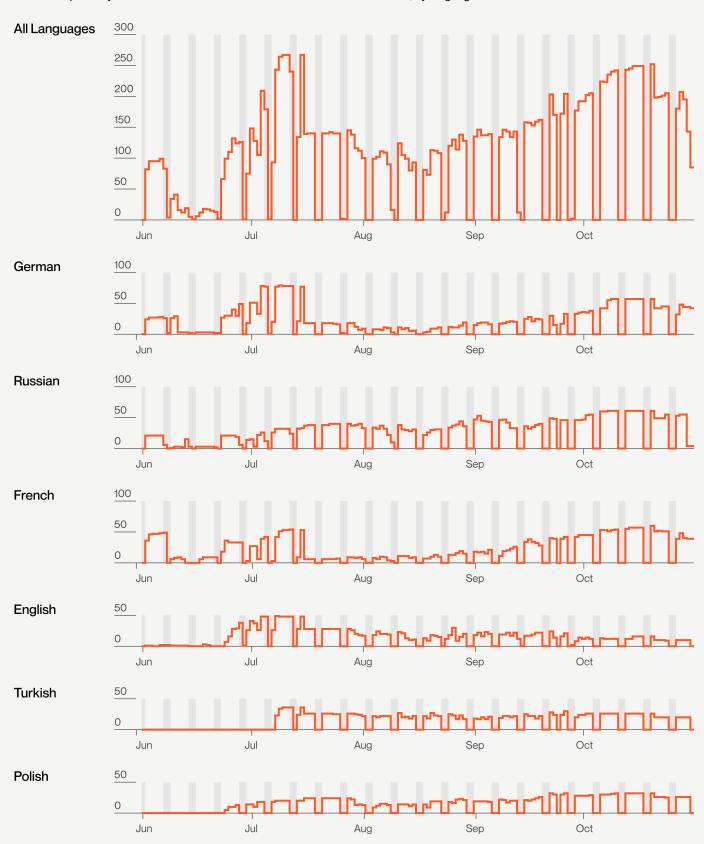


Figure 1: Posts by language between June and October 2024

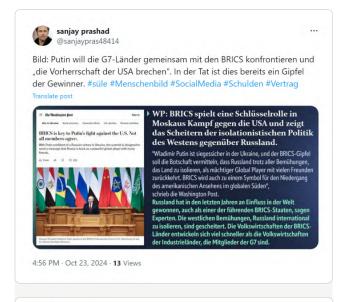
Media Formats and Content Analysis

The accounts post three types of media content: videos, GIFs, and images. The GIFs and images are often similar, with most GIFs showing a static image in a short, looping format. The images and GIFs contain lengthy texts primarily attributed to politicians, public figures, or reputable Western media.

The videos are more complex. Typically compiled from various internet-sourced clips, they feature an Al-generated voiceover with subtitles in the target audience's language. These videos generally last 28 to 29 seconds and use a variety of formats and styles repeated in series and occasionally across different languages. This suggests that the actors produce this content in batches.

Each post includes a brief caption—typically one sentence—followed by a series of hashtags. The primary focus is on the attached media files rather than the text, which often include provocative or attention-grabbing phrases to enhance engagement.

We identified various errors and inconsistencies in the media content distributed in every language. For instance, some videos' subtitles unexpectedly switch languages, English videos feature narration with a Russian accent, and many videos end abruptly mid-sentence. The media content for French, German, Turkish, and Polish audiences shows clear signs of automated generation. This includes Al-produced voiceovers, which often result in unusual prosody, and subtitles based on these voiceovers. These subtitles usually contain numerous grammatical and lexical errors, indicating a high degree of automation in the video production process.



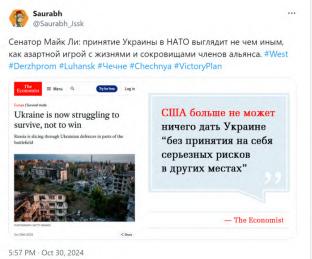


Figure 2: Screenshots from X of posts by the network in German and Russian. Both illustrate a common tactic: quoting reputable Western media as sources to emphasize negative narratives. The German post (top) includes an image based on an article by the Washington Post, referenced in the post's caption (translated). The Russian post (bottom) features a translated screenshot from an article by The Economist. These websites published both articles. This practice of referencing media reports—whether fabricated or authentic—yet presented in a distorted context is a hallmark of the campaign. Both posts use trending hashtags to amplify the story.

(Source: X top, bottom. Archived links: 1, 2)







Figure 3: Screenshots from X of posts by the network in German (top) and French (bottom): both convey the same narrative regarding Ukraine's shortage of soldiers and the impending mobilization of women. The posts feature lengthy texts accompanied by visuals of President Zelenskyy. Both cite The Washington Post as the source of the story, but this attribution appears in the text of the visual rather than in the caption. Both posts use trending hashtags to amplify the story.

(Source: X top, bottom. Archived links: 1, 2)

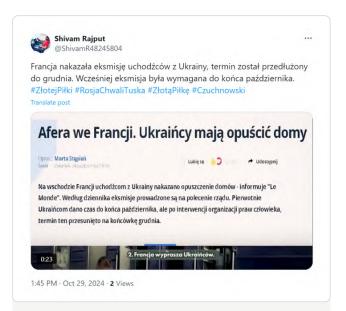




Figure 4: Screenshots from X showing two videos by accounts from the network: a Polish-language video post features an article from Polish media, utilizing the same tactic to emphasize media references for the stories. Similarly, a Turkish video begins by citing the French media Le Monde, attributing the escalation of the situation in the Kursk border region to NATO's actions. Both posts use trending hashtags to amplify the story.

(Source: X top, bottom. Archived links: 1, 2)



Table Cross-Referencing the Network's Content Production by Language

	English	German	French	Polish	Russian	Turkish
Content	Mainly anti- Ukraine narratives. Critiques of U.S. military aid, sanctions on Russia, and a heavy focus on U.S. politics (U.S. elections).	Mainly anti- Ukraine narratives. Critiques of sanctions against Russia and narratives indicating how the German economy is failing.	Anti-Ukraine narratives. Content praising Russia, claiming that Ukraine is in a very difficult situation and French people are against the war.	Critiques of NATO. Anti-Ukraine narratives. Content praising Russia.	Anti-Ukraine narratives. Content underlining how Ukraine is struggling and its economic and military difficulties.	Content about Turkish politics, praising Turkey's intent to participate in BRICS. Content underlining Turkey's weak economy to criticize its relations with the U.S.
Post Structure	Short, error-free sentences. Cross-account tweet replication with minor changes in copy. Numerous unrelated hashtags are used in the copy of the posts; the sequences are frequently altered.	Cross-account tweet replication with minor changes in copy.	Cross-account tweet replication with minor changes in copy.	Cross-account tweet replication with minor changes in copy.	Cross-account tweet replication with minor changes in copy.	Cross-account tweet replication with minor changes in copy.
Type of Content	Videos, images, GIFs	Videos, images, GIFs	Videos, images, GIFs	Videos, images, GIFs	Images and GIFs, a few videos	Videos, images, GIFs
Irregularities	Some videos have Turkish subtitles (likely by mistake). The voiceover is by a female narrator with a noticeable Russian accent.	Indications of automated content (AI voiceover on videos, odd speech prosody).Typos/ grammar errors in video subtitles (autogenerated).	Indications of automated content (AI voiceover on videos, odd speech prosody).Typos/ grammar errors in video subtitles (autogenerated).	Indications of automated content (AI voiceover on videos, odd speech prosody).Typos/ grammar errors in video subtitles (autogenerated).	Videos are rarely used. The visuals often contain logos of or quote Western media.	Indications of automated content (AI voiceover on videos, odd speech prosody)

Figure 5: Content strategies by target language.



Amplification Tactics

The <u>tactics identified in our initial report</u> remain consistent over the analyzed period. The actors continue to exploit **X**'s blue checkmarks and trending hashtags feature to artificially boost content visibility for target audiences.

Blue Checkmarks and Trending Hashtags

A primary tactic for amplifying the campaign's reach is utilizing verified X accounts for content dissemination. The blue checkmark verification enhances visibility in search results and adds credibility to otherwise anonymous accounts. However, we observed certain inconsistencies, as some accounts were verified while others were not.

Over half of the network comprised verified X accounts, indicating they have paid for the blue checkmark at least once through a monthly subscription. Between June and October 2024, 281 accounts—53 percent—were verified at some point. Typically, these accounts are verified before posting, indicating that this strategy boosts visibility. While many accounts lose verification shortly after payment, some retain it longer. We estimate that X has generated at least \$2,200 in profit from these verifications.

The second amplification tactic consistently employed by the network is hashtag hijacking.

Each post concludes with hashtags relevant to the target countries and in the local language. These hashtags are trending on the day the posts are published. These hashtags differ significantly from the political content promoted by the network. While hashtag hijacking for political propaganda is not new, this campaign effectively leverages the popularity of trending hashtags to boost content visibility.

Our findings align with the <u>February 2024 German Ministry of Foreign Affairs report regarding the Doppelganger operation</u>. The report highlighted that the campaign has consistently used trending hashtags on **X**.

Occasionally, the network used trending hashtags in posts irrelevant to the target market. These inconsistencies allowed us to identify the network's activity in languages such as Polish and Turkish. Overlapping hashtags across different languages suggests a common operational framework within the campaign.

The Network: Coordinated Activity in Clusters

The number of accounts activated in the campaign has more than doubled—from 250 to 530— since the release of our first report on October 31.

All accounts in the network exhibit clear markers of CIB, including synchronized posting, sharing near-identical content, switching between clusters of accounts, and using repetitive keyphrases. Each cluster exhibits profile similarities, such as common branding, closely aligned creation dates, and similar contact information, making them easily identifiable as part of an integrated ecosystem.

Despite evident signs of coordination, X has yet to suspend the network and is taking significantly longer to detect some accounts. As of October 31, 2024, 36 percent of accounts are active, with 192 out of 530 remaining online. One hundred eighteen accounts that posted content as early as June or July are still open. While many of these accounts continue to post, 70 have ceased posting activity between June and September 2024 but have not been deplatformed. These findings suggest that X systematically fails to detect the network's activities promptly, allowing a significant percentage to remain online for months.

Coordinated Posting

We observed consistent and coordinated posting activity among accounts that shared similar post content, both within the same language and across different languages, and on topics unrelated to the political campaign.

Coordinated Posting Within the Same Language

Coordinated posting is a crucial feature of the campaign. Numerous accounts are activated in daily batches to generate identical or nearly identical posts, which are published in rapid succession using the same media content. This approach results in identical timelines across different accounts. The brief time interval between the posts and minor variations in the copy appear to be strategies designed to evade X detection of automated activity.

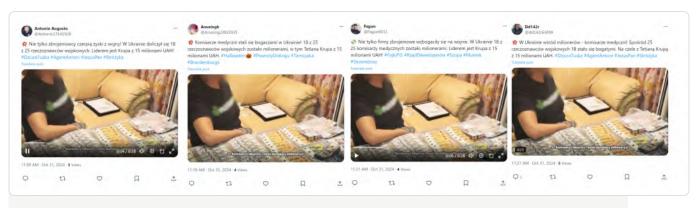


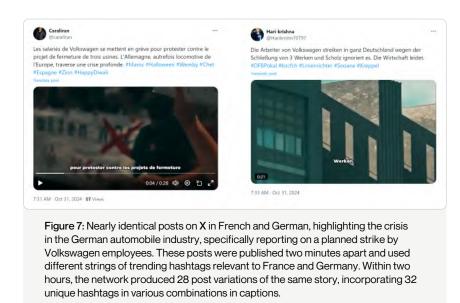
Figure 6: Coordinated postingon X in Polish language: Four accounts in the cluster shared the same video on October 31 at 11:09 a.m., 11:18 a.m., 11:27 a.m., and 11:31 a.m. Each shares the same media content twice daily (mostly videos), with slight variations in the post copy. The hashtags vary in each post, featuring a different set to boost visibility across various communities.

(Source: X 1, 2, 3, 4. Archived links: 1, 2, 3, 4)



Coordinated Posting Between Languages

The coordination across languages featured nearly identical captions and matching media content posted almost simultaneously by different linguistic clusters. We observed consistent coordination between the French and German clusters throughout the period. These accounts typically generate multiple posts daily, slightly varying the caption in the target languages and using a range of hashtags.



Quotes, Proverbs, and Motivational Phrases

(Source: X 1, 2. Archived links: 1, 2.)

Before their involvement in the campaign, some of the accounts typically posted a single sentence in English and other languages as text-only content. These posts often featured phrases such as proverbs or motivational phrases. After this initial post, the accounts would remain inactive before sharing campaign-related content. We identified over 6,500 dormant accounts within the network by analyzing several quotes, detailed in the section "The Broader Ecosystem." Of these accounts, 21 percent have been used in earlier phases of the campaign, from September 2023 onwards, but have since become inactive. Despite evident markers of coordinated posting activity, X has not de-platformed the broader network, which remains operational to this day.

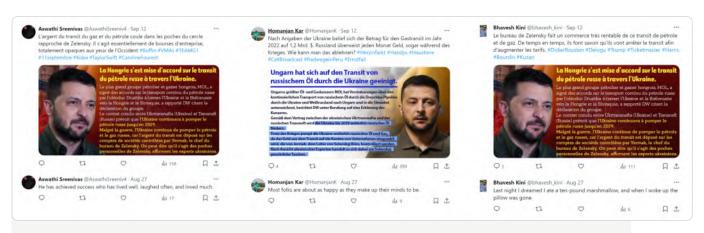


Figure 8: Three X accounts from French and German clusters, each publishing inspirational phrases on August 27 before joining the campaign in their respective languages two weeks later, on September 12. In total, 18 accounts from the analyzed network began their campaign activity with a lifestyle quote in English on August 27.

(Source: X 1, 2, 3. Archived links: 1, 2, 3)



Coordinated Activity Across Other Topics

Some accounts varied their posting topics, initially focusing on cryptocurrency and NFTs. They promoted specific coins, digital assets, and NFT marketplaces before shifting focus to political campaigns. Others began to promote Web3 apps and cryptocurrencies after pausing their posts related to the campaign. This shifting between topics suggests that certain assets are used across multiple promotional campaigns, both commercial and political.

Accounts Clusters

Various account clusters have been mobilized as part of the campaign, exhibiting shared characteristics and, in some cases, a common origin. The posting activity varies among the accounts, even though the content strategy remains consistent across the clusters. Our analysis has identified four distinct clusters active in the campaign since June 2024, each exhibiting specific characteristics.

- Anonymous accounts using celebrity profile photos
- Older accounts (likely hacked or repurposed)
- Accounts using NFTs as profile photos
- Other accounts (uncategorized)

Cluster Using Celebrity Profile Photos

The first group features accounts with profile photos of Hollywood celebrities. Most of these accounts begin their campaign activity as verified accounts, typically displaying the blue checkmark within the first month but often losing it afterward. We observed numerous cases in this "celebrity cluster" that share identical profile photos and close creation dates. The creation dates of these "celebrity" accounts vary: some were launched in January and February 2024, likely created for the campaign, while others are older accounts, likely rebranded before starting their campaign activities. Many of these accounts use Indian names.



Figure 9: Screenshots of four X accounts featuring profile photos of Hollywood actors Brad Pitt, Matt Le Blanc, and Andrew Garfield. At least 60 accounts showcased images of male celebrities, with many using the same photos across multiple accounts; for instance, at least 12 accounts in the cluster utilized the same two photos of Brad Pitt.

(Source: X 1, 2, 3, 4. Archived links: 1, 2, 3, 4)

Cluster of Older Hacked or Repurposed Accounts

This group of accounts appears to consist of assets likely expropriated from their original owners. The accounts retain the original profiles, contact details, and cover photos of real individuals. Some older posts by the original authors are still visible, further evidencing the accounts' true origins. The initial lists of followed accounts often remain unchanged, suggesting the actual owners' country of origin. Additionally, there are significant discrepancies between the original languages used by the accounts before they were taken over and the languages in the campaign-related content since June 2024.



Our analysis shows that accounts from various countries, including Brazil, India, Nigeria, Spain, Tunisia, and the U.S., were hacked and re-purposed for the campaign. Of the 530 active accounts since June 2024, at least 90 were identified as hacked, though the true number is likely higher. We classified an account as hacked only if it continued to display the original owner's photos, contact information, or previous posts. In some cases, hacked accounts may have had their activity cleared before being used in the campaign. In several cases, we verified the identities of owners of the compromised accounts, such as one Indian user whose profile photo and bio remained intact after the campaign launched, enabling us to trace him on another social media platform.

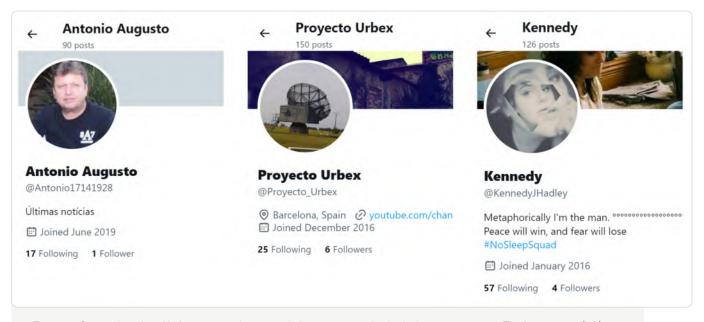


Figure 10: Screenshots from X of expropriated accounts belonging to actual individuals or organizations. The first account (left) was created in June 2019, posting in Portuguese in 2022. These posts have remained since the account's takeover. It primarily follows Brazil-based accounts, reflecting its original owner's location. The second account (middle) previously belonged to a Spanish vlogger and still carries a link to the user's authentic YouTube channel in its bio. The account follows mostly Spanish and Catalan accounts. A Spanish post from 2017 remains visible. Since June 2024, the account has published political content in Russian. The third account (right), created in January 2016, retains its original profile and cover photos, posts in English from 2016, and follows U.S.-based accounts. It was reactivated in June 2024, posting in French and Turkish since then.

(Source: X 1, 2, 3. Archived links: 1, 2, 3)



Figure 11: Screenshots from X showing an account created in January 2016 (left). Its first post in English was published on January 12 (right). The original cover photo, profile picture, and initial post remain visible. After eight years of inactivity, the account was reactivated on June 3, 2024, and began posting campaign-related content in French. It switched to Turkish in July, maintaining activity in this language until October 31.

(Source: X. Archived link: 1)

Indian Username Cluster

A group of old accounts appears to have been utilized as assets for posting content in other campaigns, such as those related to cryptocurrencies. While some may have been expropriated from their previous owners, others display no posting activity, leaving their origin unclear. Most of these accounts have Indian usernames and feature profile pictures of male individuals. Some accounts are older, while others were created between January and February 2024, likely as assets for campaigning. Similar to the Hollywood celebrity cluster, some analyzed photos featured Indian actors.

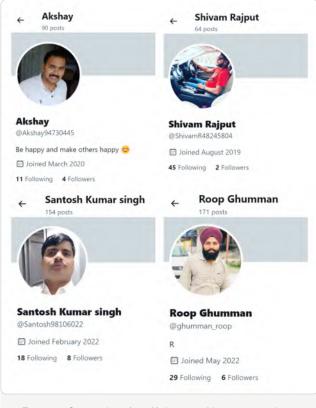
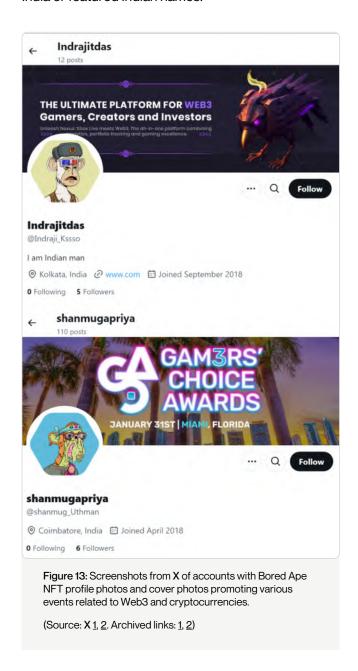


Figure 12: Screenshots from X showing old accounts with Indian names and profile photos. These accounts primarily follow other Indian accounts, indicating their origins. Screenshot 1(top left) features a photo of Indian actor Joseph Vijay Chandrasekhar, while the individuals in the other screenshots (2, 3, 4) could not be identified. Unlike other hacked accounts, most analyzed Indian accounts show no posting activity prior to the campaign. In some cases, posts from the original author remain visible (screenshot 2). This account has been active since September 2024, posting content in Polish. Many accounts switch between campaign languages. For example, screenshot 3 began posting in Russian in July and switched to French in September.

(Source: X 1, 2, 3, 4. Archived links: 1, 2, 3, 4)

Cluster of Accounts Using NFTs as Profile Photos

This cluster uses NFT avatars as profile pictures. The accounts were created in Q2 2018. We identified over 80 similar accounts within the sample of 520. These accounts displayed Bored Ape NFT profile photos, and many had previously promoted cryptocurrencies before being involved in the Doppelganger campaign. Similar to the earlier cluster, we identified a connection: some accounts contained bio information related to India or featured Indian names.





Clusters of Other Accounts: Similar Bios & Branding

The branding identity among some clusters of accounts is strikingly similar. For instance, several old accounts have almost identical text in their bio sections. One cluster referenced NFTs and digital trends using similar phrases. In our sample, at least 20 accounts displayed nearly identical wording in their bios and listed the same websites in their contact details.



Figure 14: Screenshots from X of accounts with near-identical bio information and identical location. The similarity suggests these accounts might not only be participating in the political campaign but could also be part of another coordinated effort to promote specific topics, products, or services like NFTs or cryptocurrencies.

(Source: X 1, 2, 3. Archived links: 1, 2, 3)

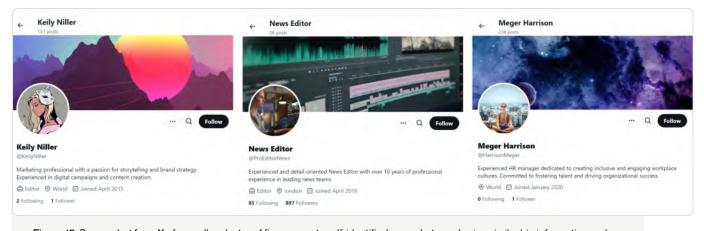


Figure 15: Screenshot from X of a smaller cluster of five accounts self-identified as marketers, sharing similar bio information and content before being activated on the Doppelganger campaign.

(Source: X 1, 2, 3. Archived links: 1, 2)



The Broader Ecosystem: Dormant Accounts from Earlier Phases

The network of 530 accounts is part of a broader ecosystem of inauthentic X accounts. Some accounts were used in earlier phases of the Doppelganger campaign but have since become inactive. By testing different combinations of key phrases from the content of some analyzed accounts' posts, we were able to map out a larger portion of this network.

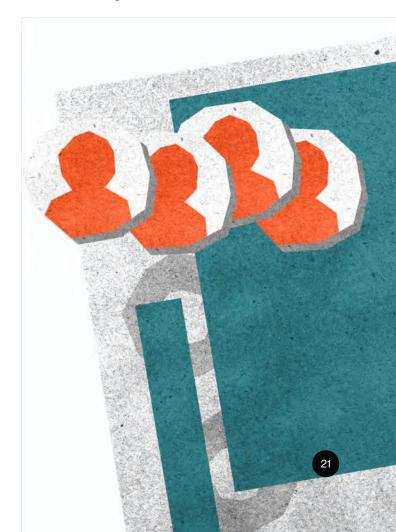
- We observed that many accounts in the sample began by posting random key phrases in various languages, including English, French, German, Polish, Italian, and Ukrainian. These posts often featured popular proverbs or idioms in the target language or randomly selected inspirational phrases related to various topics in popular psychology, such as relationships, careers, work-life balance, building self-esteem, and emotional intelligence. Searching for these key phrases revealed additional posts from similar accounts, significantly expanding the network.
- Campaign posts from certain accounts often used repetitive phrases in their captions. By searching for these phrases, we uncovered more relevant accounts.

We analyzed a sample of over 110 key phrases across various languages, mapping a network of nearly 6,500 accounts. After publishing an initial post of a proverb or inspirational phrase, most accounts we discovered typically remain dormant. Approximately 5,000 accounts did not create original content after their first post and were not used in the Doppelganger operation. Some dormant accounts occasionally showed bursts of random retweeting across various topics. Their engagement with unrelated content suggests these accounts could be repurposed for other campaigns, such as promoting cryptocurrencies.

At least 1,400 accounts have shared at least one piece of political content linked to the Doppelganger operation in English, German, French, Hebrew, Italian, Ukrainian, and Russian.

Their posting activity differs from that of the analyzed network: they typically publish one political post before becoming dormant. Most were created between November and December 2023. Many were activated for the campaign in January and February 2024; however, we found earlier posts dating back to May 2023.

The mapped network likely represents only a small part of the latent ecosystem, as we could not capture all key phrases from various account clusters and frequently discovered new ones. Compared to our analyzed sample from June to September 2024, the language distribution appears uneven, suggesting content was targeted at different audiences.



Characteristics of the Campaign's Earlier Phase



Pro-Kremlin Narratives

Amplifying similar pro-Kremlin narratives



Tactic of Trending Hashtags

Using trending hashtags as a consistent tactic across languages.



Dormant After One Post

Accounts becoming dormant after their initial post



Pivot to Long-Term Assets

Pivoting from relying on large networks of one-time assets—accounts that publish once and then become dormant—to using fewer assets that post more consistently, specifically the clusters analyzed since June 2024.



Adoption of Verification

An absence of verified accounts before June 2024. This may indicate that X verification is a new tactic aimed at enhancing legitimacy and ensuring sustained involvement in the campaign.



Dominance of English Posting

Most accounts posted in English—58 percent, or 850 accounts. We found posts in other languages, including French, German, Hebrew, Italian, Polish, Russian, and Ukrainian. After June 2024, some languages appear to have been discontinued.



Commenting-Only Strategy

A small number of accounts posted comments exclusively. This appears to be a separate content strategy to infiltrate specific online spaces.

Figure 16: An infographic detailing the characteristics of the campaign.

Many of the accounts in this network were used as disposable, one-time assets, yet there were clear markers of CIB that the platform had not detected until now. A consistent content strategy, identical text in posts, and common branding across specific clusters made it relatively easy to identify the earlier stages of the campaign. As of October 2024, the majority of the identified network of 6,500 accounts remains active, nearly a year after being used in the political campaign. This network could be reactivated at any time to produce similar content.

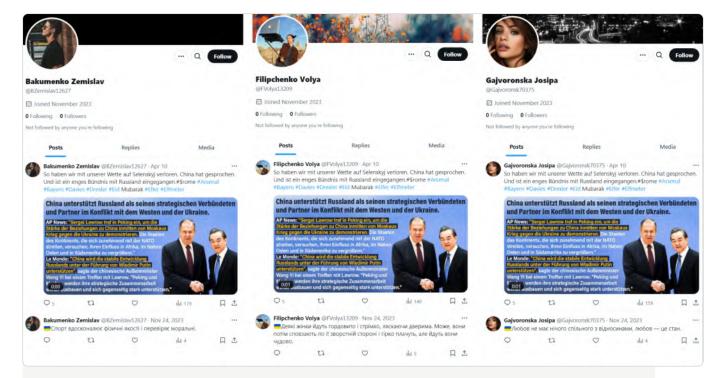


Figure 17: Screenshots from X showing coordinated posting in earlier campaign phases: three accounts published the same keyphrase in Ukrainian on November 24, 2023. The accounts remain dormant for months and are reactivated on April 10, 2024, posting in German about China's support for Russia. These three accounts are still active as of October 2024, months after being activated for the campaign, and may be used as assets in the future.

(Source: X 1, 2, 3. Archived links: 1, 2, 3)

Evolution of an Inauthentic X Account

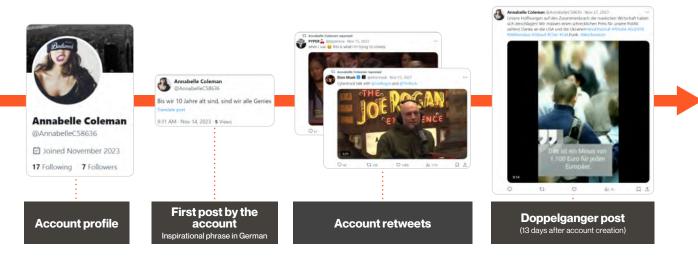
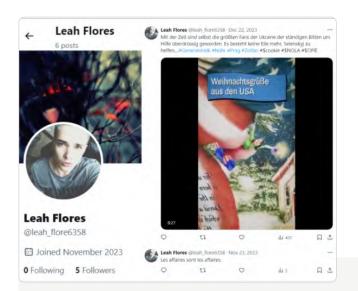


Figure 18: Timeline with Screenshots from X illustrating the evolution of a Doppelganger account: The account was created in November 2023. On November 14, the account posted an inspirational phrase in German. On November 15, it retweeted multiple seemingly random accounts. On November 27, it posted a video criticizing Germany's financial aid for Ukraine. No further activity was observed throughout 2024. The account is still active and could be used in the future.

(Source: X. Archived links: 1)



Examples of Dormant Accounts



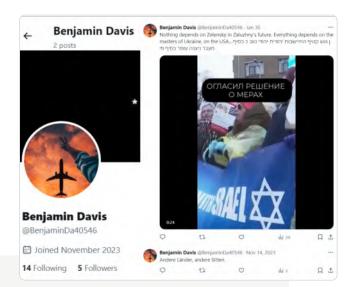


Figure 19: Screenshot from X of accounts from an early campaign iteration in 2024. The accounts displayed limited activity, typically posting just once following an initial post containing an inspirational phrase. After weeks or months of inactivity, the accounts would share political content before becoming dormant again. Notably, there was inconsistency in the language of the inspirational phrases compared to those in the subsequent campaign posts. The account in screenshot 1 (left) uses French before switching to German. The account in screenshot 2 (right) shares a German proverb and later posts in English/Hebrew.

Source: X 1, 2. Archived links: 1, 2)

Examples of Accounts with Mismatched Profile Names and Pictures

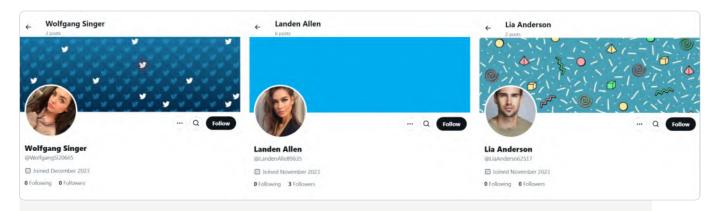


Figure 20: Screenshot from X showing three examples of inauthentic accounts used in earlier phases of the campaign. These accounts often featured profile photos of models to create fake personas. Reverse image searches show that some of these images primarily originate from Russian websites, indicating the actors' origins. Additionally, profile names and photos were frequently mismatched, with male images being paired with female names and vice versa. All three accounts shared campaign-related content in German in December 2023 but became dormant after their initial posts. All three accounts remain active online.

(Source: 1, 2, 3. Archived links: 1, 2, 3)

Insufficient Response to the Campaign by X

Despite clear indicators of long-term coordination among individual accounts, content themes, and the network as a whole, X's responses to the operators' activities have been inconsistent and selective. The platform's efforts to combat the campaign have involved de-platforming certain accounts while neglecting to address the broader ecosystem. Since our initial report, the network identified in June 2024 has expanded by over 50 percent and has continued its activities without restriction, even adding a sixth language.

Although the platform has removed verification badges and continually suspends accounts, new verified assets continue to join the campaign, generating additional revenue for X. Deleting specific accounts will not stop the campaign; only stricter content moderation can effectively monitor it.

Once again, X's trending hashtags feature is being exploited for pro-Kremlin propaganda. Hashtag hijacking is a notorious tactic used to spread disinformation and scams.

The campaign continuously amplifies politically driven narratives to reach new audiences by leveraging the algorithm's prioritization of trending topics. Although the posts generate very limited engagement and reach, manipulating the trending algorithms remains an effective strategy for gaining traction. Improved content moderation around trending hashtags could help reduce the influence of similar campaigns in the future.

X has failed to de-platform dormant accounts within the broader ecosystem of Doppelganger assets active in the campaign in 2023 and 2024. The network of 6,500 mapped accounts still exists; its actual size is likely even larger. Although only 21 percent of the network—1,400 accounts—have published political content, these assets can be reactivated at any time to produce similar content.

Conclusion

The pro-Kremlin Doppelganger operation has been active since 2022. X is just one of the platforms where this campaign is strategically executed through coordinated networks of inauthentic accounts that target audiences in the EU. The operation persists on X primarily due to platform-specific features, such as trending hashtags and paid blue checkmarks, which increase the visibility of the content published by these anonymous accounts.

Our five-month observations show that the platform appears to systematically fail to intervene and stop the network. While the analyzed network is not currently running any paid advertisements, X continues to profit from its activities by monetizing verification badges, which is a crucial tactic of the current operation phase.

The content strategy has evolved from sharing links to external websites to focusing on keeping content consumption within the platform, engaging audiences through various media formats. Videos are increasingly becoming the preferred medium for spreading disinformation. Additionally, AI technology has made generating multilingual audiovisual content significantly easier for content producers. We can expect to see more developments in this approach in the future.

Disclaimer:

This report reflects the authors' views and is based on data available up to the date of publication. Subsequent changes may not be incorporated. This document is a product of professional research.

Copyright © 2024 Reset Tech. All rights reserved.

This report and its contents are copyrighted under the CC BY-NC-ND 4.0 Deed (Attribution-NonCommercial-NoDerivs 4.0 International). For permission to use the content outside this license, please contact hello@reset.tech.



Reset ·Tech

Verified Disinformation:

How X Profits From the Rise of a Pro-Kremlin Network

Dec 2024