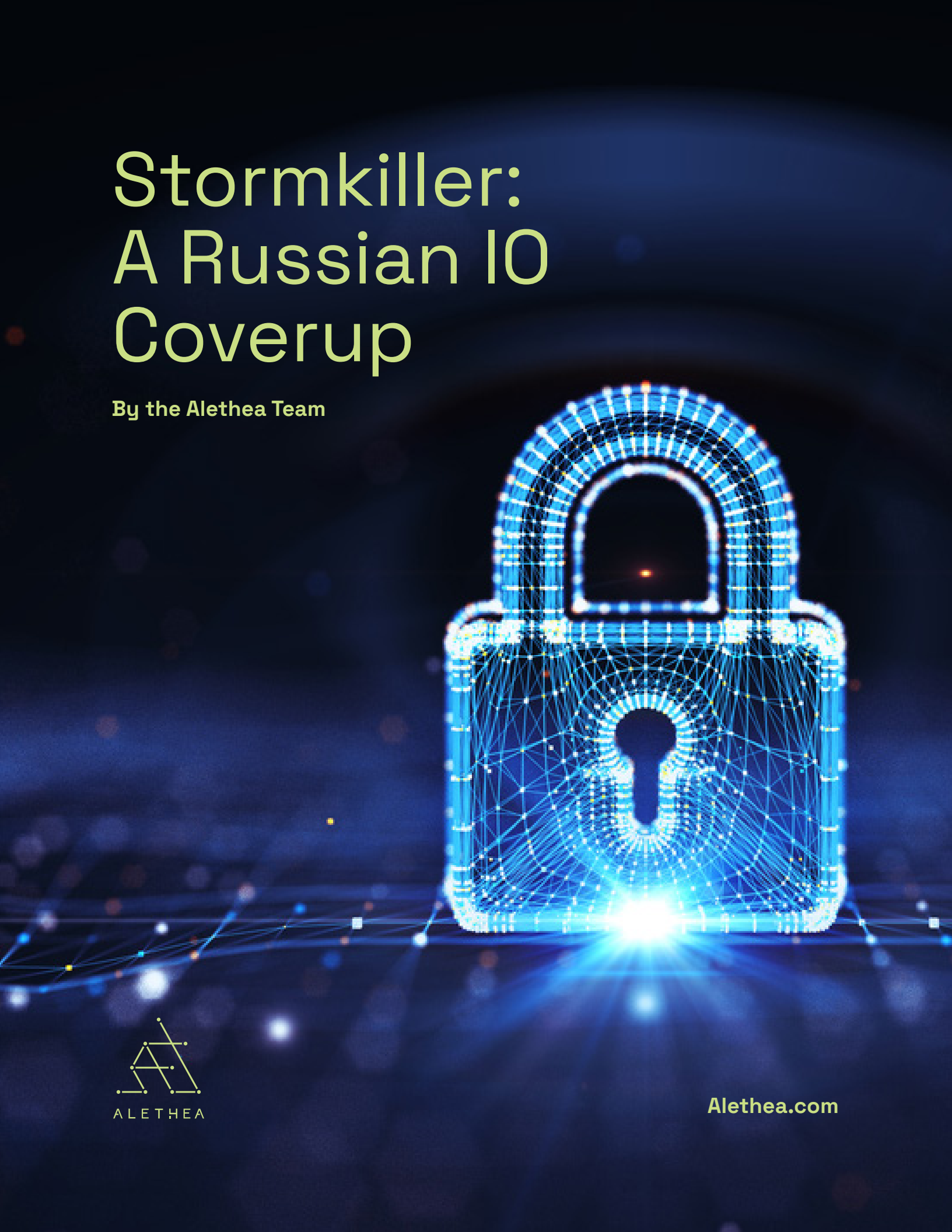
Stormkiller: A Russian IO Coverup

By the Alethea Team



ALETHEA

Alethea.com

EXECUTIVE SUMMARY

Alethea identified a network of X accounts assessed as a subset of Russia's broader network of accounts used in ongoing influence operation efforts, including those seeking to impact the 2024 Presidential Election.

While investigating this network, Alethea observed **a shift in the behavior of some accounts**, potentially reacting to the September 4, 2024, DOJ affidavit which implicates Social Design Agency—a Russian firm suspected of operating at the behest of the Russian government—in operating the influence campaign known as Doppelgänger, known for its use of cloned websites of legitimate news outlets. This shift included **faked claims by prominent disinformation experts**, including Eliot Higgins, founder of Bellingcat, and Christo Grozev, the former lead Russia investigator at Bellingcat. Often, this apparent new effort to cast doubt on Russia's involvement in these influence campaigns **shifted the blame to Ukraine**—who relies on democracies for financial and geopolitical support and is often itself a target of the campaign.

Russian efforts to mischaracterize expert analysis of its malign activity, particularly those including the names given to these operations by researchers, is **a deflection tactic not yet documented in analyses of related influence operations.** Alethea has dubbed this approach "Stormkiller," based on the Microsoft "Storm" nomenclature used for tracking Doppelgänger-related groups, and the network's apparent shift to posting content with the goal of "killing" the DOJ's allegations.

Alethea has otherwise observed this network spreading narratives denigrating U.S. Vice President Harris, NATO, Ukraine, and other key international organizations and alliances. While the network continues to target Ukraine and Vice President Harris—often with content that contains racist and misogynist narratives—the shift since September 4 suggests that influence operations have assumed a new focus: deflecting the blame for their foreign influence operations targeting the U.S. and Europe.

Based on account behavior and content similarities, **we assess with moderate confidence that the activity is related to the operations known as Matryoshka or Operation Overload;** these influence campaigns have been associated with Doppelgänger, which has been attributed to Social Design Agency. The accounts in this network amplify original—and often misleading or explicitly false—content including videos, memes, and articles, that is originally seeded on Telegram and designed to impersonate legitimate Western news outlets or government agencies, such as the FBI or CIA.

BACKGROUND

Alethea consistently tracks Russian influence operations as part of its ongoing effort to provide insight into risks in the online information environment.

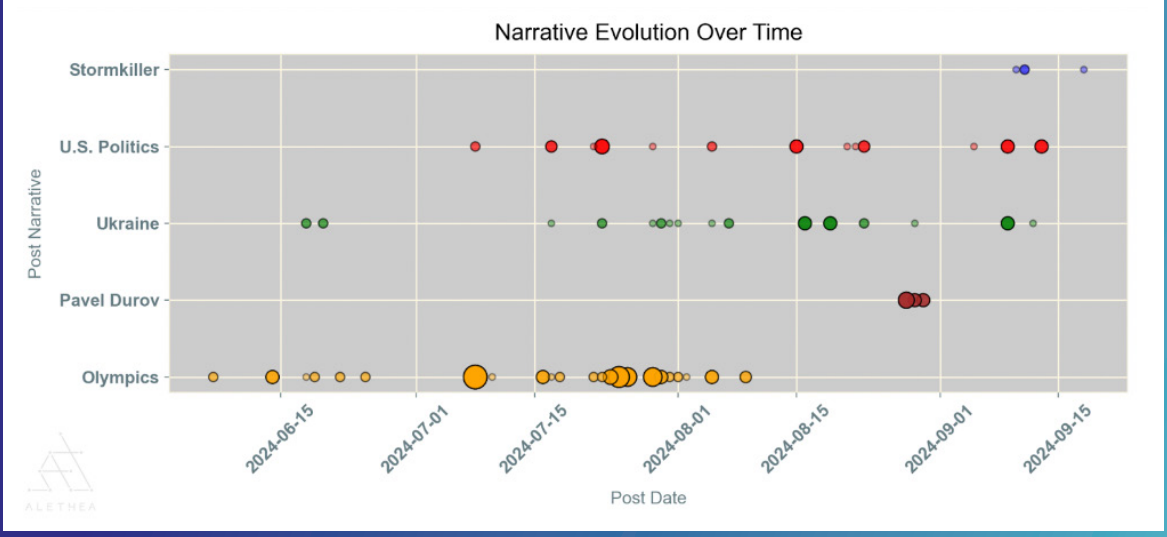
The network Alethea identified in this investigation consists of 77 accounts on X that posted 113 original, often multimedia, posts. At least 60 of these accounts both posted and amplified network content, collectively sharing 9,000 quote posts of other assets' content. Recently, the network engaged at least 420 additional accounts that were solely used to amplify content through reposts. In many cases, Alethea observed that some content was shared on Telegram prior to the content being posted on X.

As detailed in Alethea's March 2024 report, **Invisible Ink,** Russian attempts to influence elections have shifted from dividing democracies to being almost singularly focused on electing candidates that are likely to stop supporting Ukraine, or to push populations away from supporting foreign aid to Ukraine. This is evident globally, including in the United States.

Alethea has also observed that Russian influence operations have increasingly substituted traditional, large-scale means of inauthentic content production and amplification for more subtle tactics that are more likely to evade detection. For example, the Invisible Ink tactic helps the campaign to amplify content while evading detection by X.

Content

While the vast majority of the content posted by this network aligns with previously-reported trends regarding Russian information operations, **Alethea identified notable content dubbed as "Stormkiller,"** in which assets in the network almost certainly responded to the September 4 DOJ affidavit implicating the Social Design Agency in Russian influence campaigns. Other original content posted by network assets focused primarily on four categories: U.S. politics, the war in Ukraine, the arrest of Telegram CEO Pavel Durov, and the 2024 Paris Olympics. Developments in these four areas broadly corresponded to shifts in newscycle priorities, with U.S. politics and Ukraine content continuing after the conclusion of content about the Olympics or Durov's arrest:



Scatter plot of network posting activity related to this operation organized by primary narrative, showing changes in narratives over time.

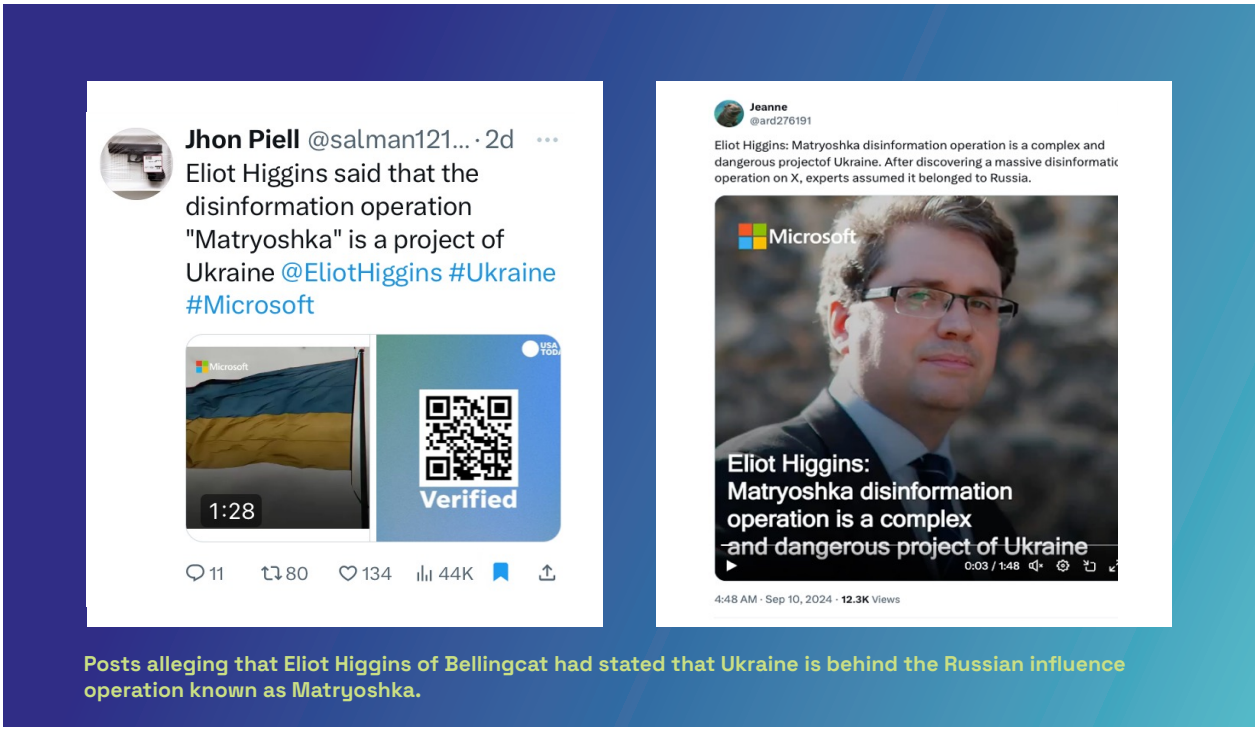
Stormkiller Content

Following the September 4 DOJ affidavit and into mid-September, Alethea observed the operation attempting to disassociate from its own influence activities, often attempting to deflect blame onto Ukraine. The operation produced content allegedly quoting counter-disinformation experts who had previously attributed Matryoshka influence operation activities to Russia, claiming these organizations had retracted their original assessments and announced they now believe Ukraine is responsible for orchestrating the campaign.

Specifically, we observed two distinct trends among this content:

- **Production and amplification of content that claims Ukraine, rather than Russia, is responsible for conducting Doppelgänger and associated influence activities.** This content alleges that experts—including Christo Grozev, formerly lead Russia investigator at Bellingcat, and Eliot Higgins, founder of Bellingcat, an organization that has previously researched Russian influence operations—had announced that they now believe Ukraine was responsible for these online campaigns.

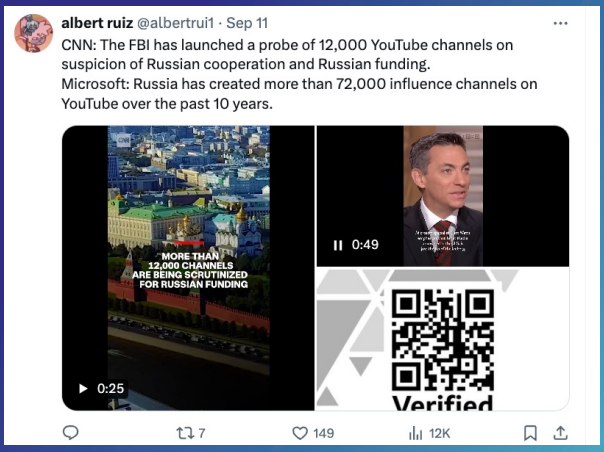
- **Automated reposting by a botnet of at least 420 batch-created X accounts.** Notably, unlike in previous stages of the campaign, the content shared by these accounts since the September 4 DOJ affidavit appears to have been amplified through synchronous reposting by a botnet—most of which has since been suspended—instead of being amplified by other active, established network assets that are less likely to be detected for coordinated inauthentic behavior.



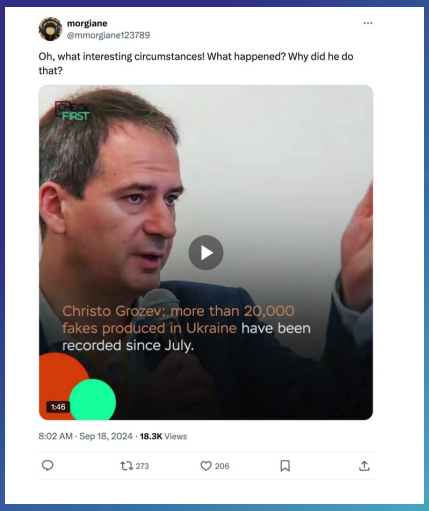
Posts alleging that Eliot Higgins of Bellingcat had stated that Ukraine is behind the Russian influence operation known as Matryoshka.

In a September 10 example of this behavior, multiple network assets shared unique content accusing Ukraine of perpetrating an influence operation against the U.S. Now-suspended network asset John Piell (@salman1212120) posted a video with Microsoft branding claiming that Eliot Higgins of Bellingcat said that the **"Matryoshka disinformation operation is a complex and dangerous project of Ukraine."** Higgins later quote-posted the video from @salman1212120 in a thread on his X account, condemning it as "fake."

Less than half an hour after the video's publication on X, it was retweeted at least 76 times in under 60 seconds by the botnet described above. Likewise, network asset Jeanne (@ard276191), which remains active at the time of writing, also shared a similar video on September 10, adding that **"experts assumed" the operation was attributable to Russia prior to Higgins's statement.**



A post by @albertrui1 contained videos reporting on Russian disinformation it claimed were produced by CNN and Microsoft, featuring Clint Watts of Microsoft.



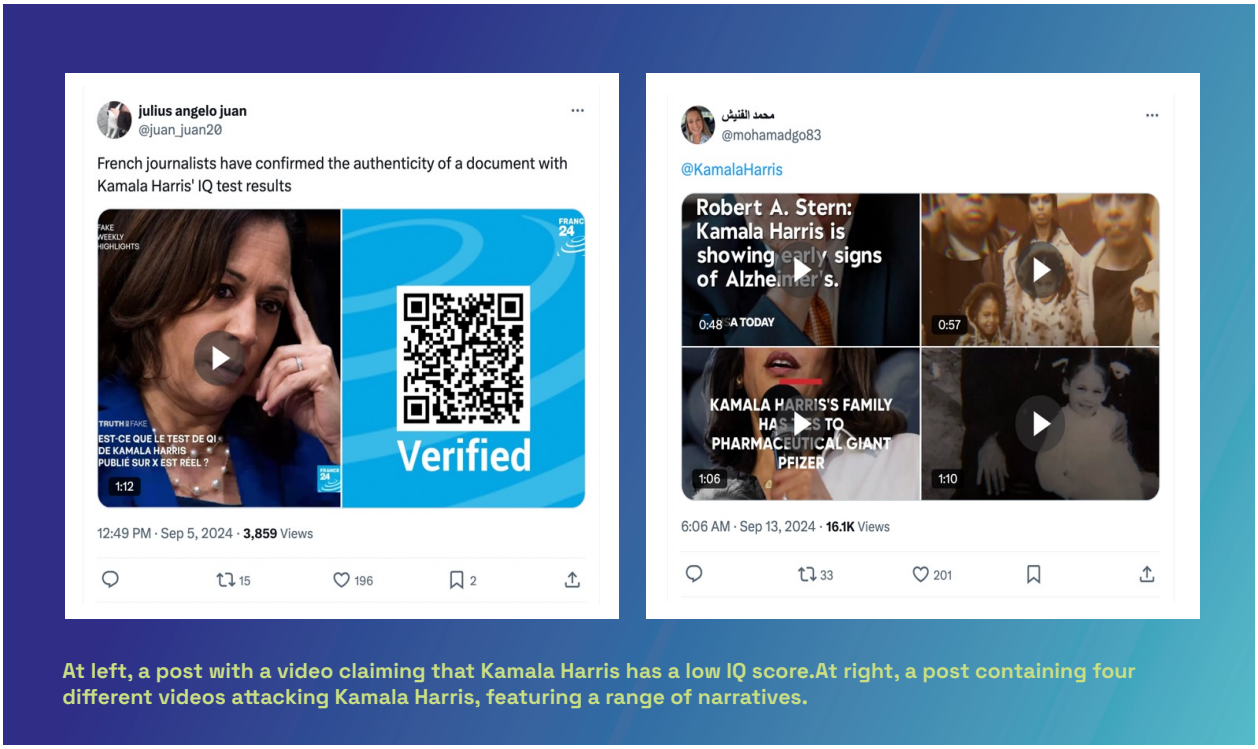
A post by @mmorgiane123789 claimed that Ukraine created the information operations attributed to Russia.

On September 11, 2024, network asset Albert Ruiz (@albertrui1), posted multiple videos and a QR code. The videos reported that the FBI had launched an investigation into 12K YouTube channels for possible Russian involvement and claimed that Russia has created over 72K channels on YouTube over the last decade for use in influence operations. This post did not receive the automated amplification that we observed on other posts.

On September 18, network asset Morgiane (@mmorgiane123789) posted a video claiming to feature information from Check First, the organization credited with exposing Operation Overload. Like the video claiming to quote Higgins, **this video claims that Ukraine is producing these fake media pieces, alleging that over 20,000 "fakes" have been produced by Ukrainian entities since July 2024.** This post also received substantial engagement—at least 273 reposts, 206 likes, and 18.3K views—from a likely inauthentic network of accounts that otherwise promoted content about cryptocurrency and NFTs.

U.S. Politics Content

For most of the reporting period, network content mentioning U.S. politics overlapped with dominant news headlines—such as the assassination attempt on former President Donald Trump—and international events—including the U.S.-Russian prisoner swap and provision of military aid to Ukrainian forces.



At left, a post with a video claiming that Kamala Harris has a low IQ score.At right, a post containing four different videos attacking Kamala Harris, featuring a range of narratives.

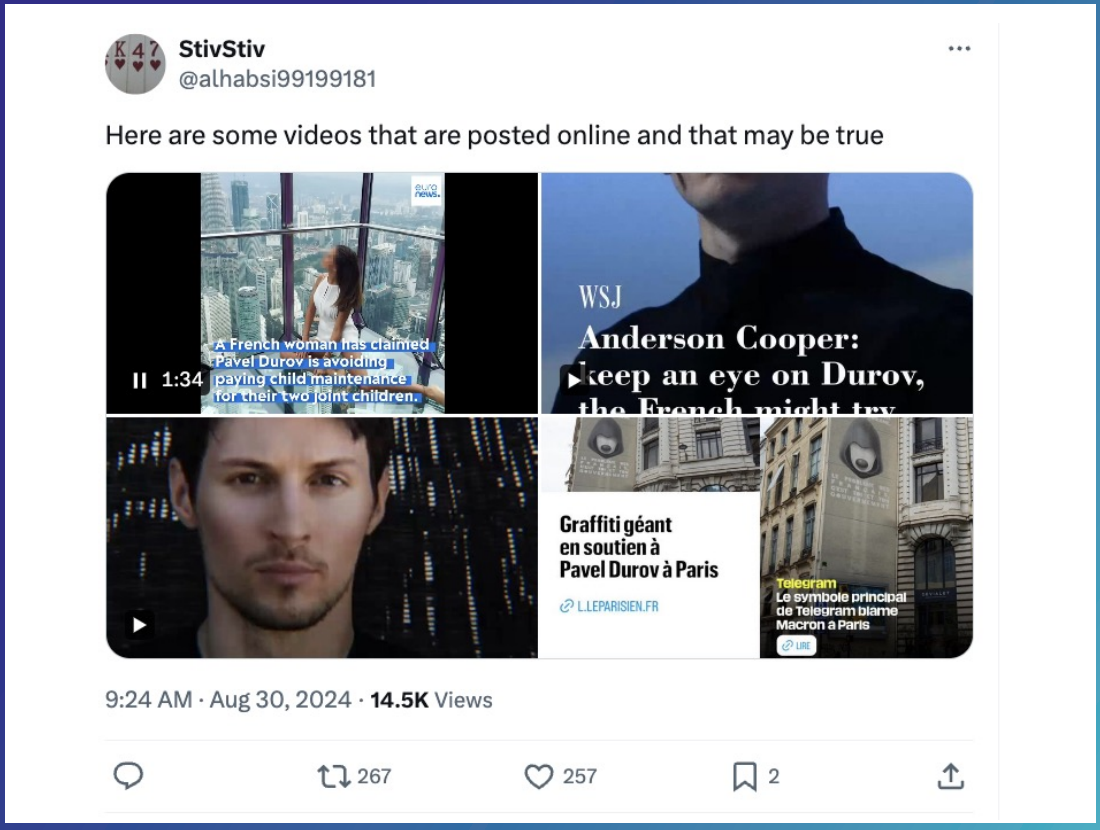
Following the conclusion of the 2024 Democratic National Convention, Alethea observed the network more directly targeting the upcoming U.S. Presidential election with a focus on content claiming that Kamala Harris is unfit for candidacy for President due to her mental state or that she had various financial and political conflicts of interest. Specifically, accusations were made that Kamala Harris has a low IQ, possibly due to previous head injuries, along with allegations that she has early signs of Alzheimer's; that Kamala Harris's family is secretly wealthy, or that she or her family have secret ties to Pfizer and "Big Pharma," which may include a financial incentive to push puberty blocker drugs for gender dysphoria; and that Harris is secretly a Marxist based on her grandfather's past Marxist teachings in Zambia and India.

Ukraine Content

A post claimed that the people of Ukraine have stopped believing in the possibility of a Ukrainian victory against Russia.

Aligning with ongoing Russian information operation priorities, the accounts in this network frequently shared content denigrating Ukraine, including claims that U.S. and NATO aid is further damaging the country and that Ukrainian refugees are committing violent crimes and disturbing the peace in Poland and other host countries. It is almost certain that these narratives sought to antagonize the relationship between NATO countries and Ukraine, between host countries and Ukrainian refugees, and between the Ukrainian population and its government.

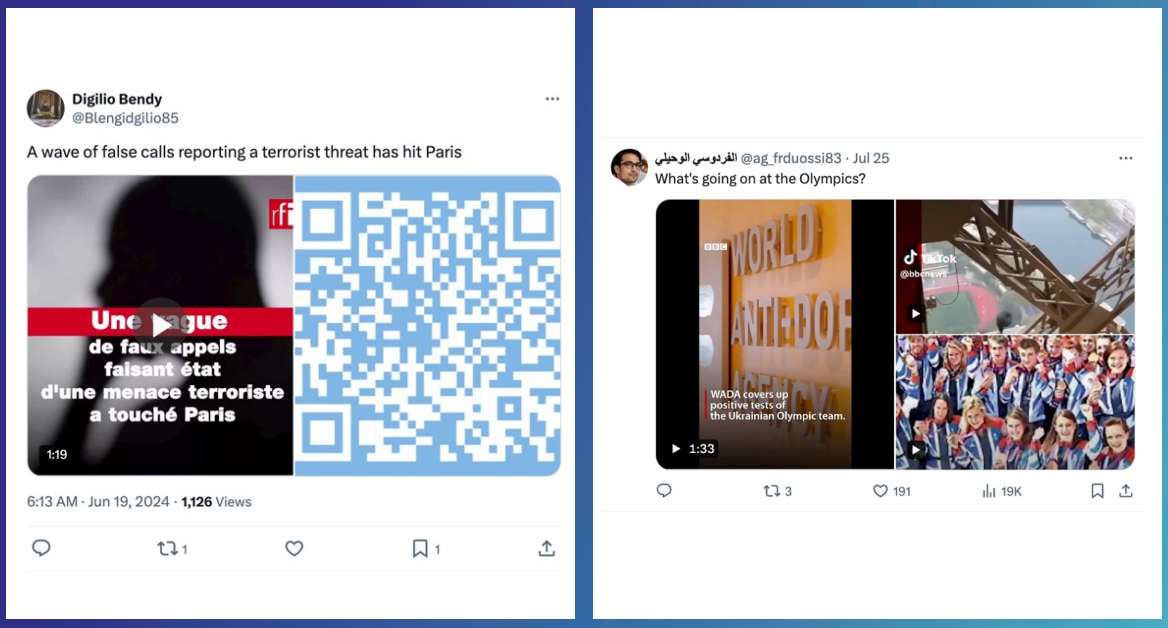
Durov Arrest Content



A post from a network asset reacted to Durov's arrest, sharing videos about him in French and English.

Following the arrest of Telegram CEO Pavel Durov upon his arrival to Paris on August 24, 2024, network assets posted content casting doubt on the lawfulness of his arrest, often accusing French President Emmanuel Macron of having an ulterior motive. There was a dense cluster of related content posted on August 28 and 29, likely in response to the announcement of charges against Durov on August 28. Among these posts were claims that the arrest was "personal revenge" or that "if Durov were gay and flying to France for dinner with his boyfriend, Macron and his gang would never have arrested him." Other posts included an inauthentic video claiming that U.S. lawyer Alan Dershowitz had earlier described the arrest of Pavel Durov as political, or another claiming that Anderson Cooper of CNN had suggested that France arrested Durov on inconclusive evidence, using his arrest for revenge against Russia for targeting France, going as far as to allege that Durov might later be murdered.

Olympics Content



At left, an example of content alleging that terrorism threatened the Paris Olympics. At right, a network asset shared a video claiming that the World Anti-Doping Agency covered up "positive tests of the Ukrainian Olympic team."

The network posted a substantial amount of content about the Olympics, as noted in other external reporting on Matryoshka and Operation Overload activity. These posts included claims that the CIA had reported a high risk of terrorism in Paris and recommended avoiding the metro, or more broadly asserted that France did not have ample control over the immigration, public health, and counterterrorism issues that threatened the success of the 2024 Olympic Games. This content spiked alongside news before and during the Olympics and naturally waned and ceased as the Olympics concluded.

About the Network

Attribution

Alethea assesses with moderate confidence that this activity is associated with the Doppelgänger-related operations known as **Matryoshka and Operation Overload**, based on similarities to previously-attributed content and on the account details and behavioral characteristics outlined below—most specifically on their use of "nested" content posting and attempts to draw attention to their faked content by replying to news outlets, fact checkers, and journalists.

We also assess with moderate confidence that at least some portion of the content originated from the actor that Microsoft tracks as Storm 1679, based on content overlaps with examples presented in recent Microsoft reporting.

Though it is unclear what specific relationship exists between these Russian influence actors, our findings support the existence of an interconnected ecosystem where content and tactics are shared among different threat actors.

The Accounts

Alethea analyzed 77 accounts, of which 70 remain active and 7 have been suspended. We assess that most, if not all, of these accounts are inauthentic based on their characteristics described below. **We suspect that as many as 56 of these accounts were originally created by legitimate users but later "hijacked" or stolen to be used for the influence operation.**

One subset of accounts in the network shared the following key characteristics:

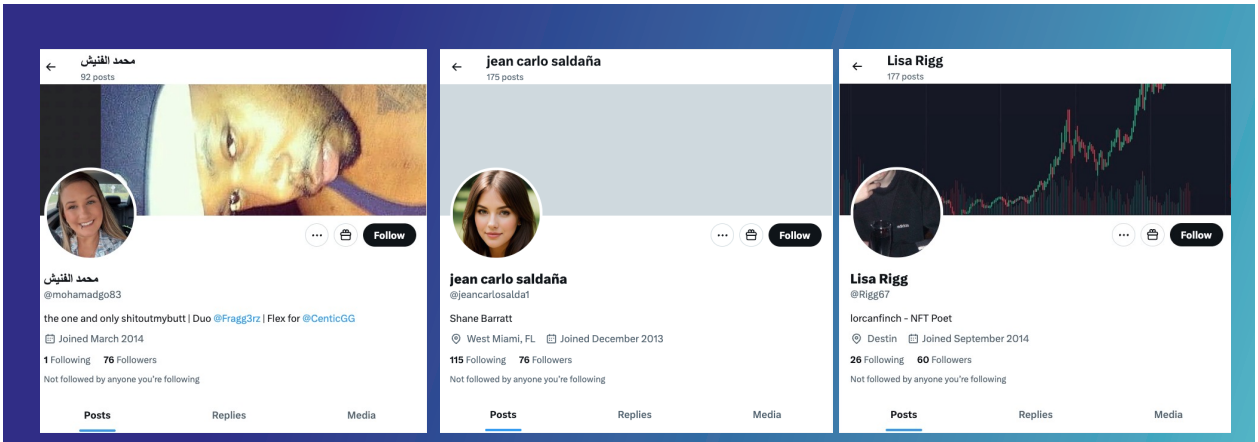
- A **years-long gap in activity,** with the cessation of activity usually starting in 2013 or 2014 and continuing until 2024, when the account resumed activity and began sharing Matryoshka content.
- **A change in the operating language of the account,** which usually corresponded to the gap in post activity, from a language such as Turkish, Portuguese, or Spanish to English.

- A **mismatch in biographical information,** including accounts' screen names, profile photos, bios, and reported locations, such as conflicting gender, multiple listed names, references to cryptocurrency, or improbable places. For example, a profile with a screen name in Arabic that says "Mohammad Al-Fneish" (@mohamadgo83) has a profile photo of a woman. Or, a profile for Jean Carlo Saldaña (@jeancarlosalda1) claims to be based in West Miami, FL, includes only the name "Shane Barratt" in its bio, and has an AI-generated profile picture of a woman.

Another set of 10 accounts shared the following key characteristics:

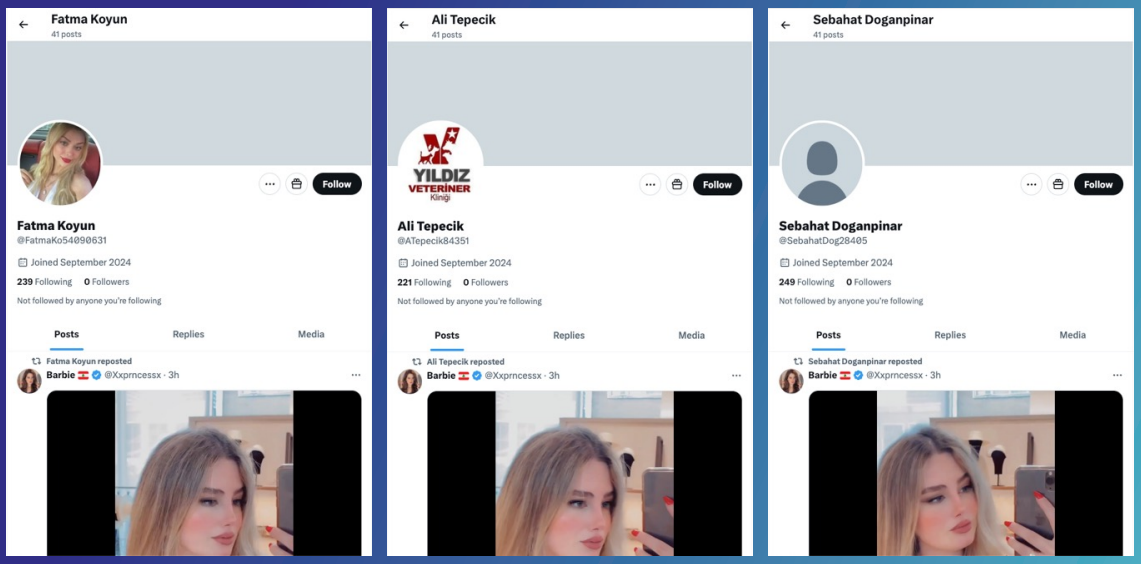
- The accounts were **created between May 5 and June 11, 2024**, with four created on May 5, and 3 created on May 22.
- The accounts have less biographical information in general, **often lacking details such as a profile bio, URL, or location.**

At least seven of the accounts used an AI-generated profile picture, while the majority used likely stolen or repurposed images, such as photos of real people, cartoon images, or other graphics.



The screenshots above display examples of account characteristics, including mismatched biographical information.

Alethea identified a suspected botnet of **at least 420 batch-created accounts that engaged in coordinated reposting**—often at the same minute—of network assets' content that all had Turkish names. Unlike the other network assets, whose names and profiles did not follow any particular pattern, these accounts all had a first and last name as their screen name, while their user handle was a combination of letters from these two names followed by five to eight digits. At least 71% (289) of these accounts had 15 characters in their X handle, though some had as few as 10. Two examples of these profile names are Herdem Arslan (@arslan_her86283) and Zeliha Meral (@zelihamera84095). In addition to amplifying network content, they reposted unrelated content in a variety of languages, including English, Turkish, Arabic, Japanese, Chinese, Hindi, and French.



Three of the reposter accounts reposted a video unrelated to the Matryoshka operation at the exact same time on September 19, 2024.

Account Behaviors

Alethea observed that the accounts in this network exhibited similar, though not completely uniform, behaviors. Unlike the Invisible Ink network, which was composed of distinct sets of "poster" and "amplifier" accounts, **the accounts in this network engaged in both posting and amplification behaviors**, sharing a multimedia post to their timeline and quote posting other assets' posts. The type of original content shared by each account varied slightly; some shared videos, others shared still images, including images containing QR codes, and still others shared a mix of videos and images.

The content posted by these accounts received more engagement than Alethea had previously observed with related influence operations, though at least a portion of the engagement appeared to be inauthentic. The 113 posts containing original content collectively received at least 1,232 reposts and 15K likes. Due to the fact that the X platform now hides the usernames of accounts that have liked a post, we were unable to assess the authenticity of the accounts who liked this content. Separately, the accounts quote-posted other assets' content as replies over 9,000 times, though the vast majority of these replies received no engagement.

Posting Behaviors

The accounts **usually shared only one original post, but sometimes shared up to three; these posts often contained multiple videos or images.** Alethea collected 113 original posts from the 77 accounts in the network, and over 9,000 quote posts of network content shared in reply to other users.

Many of the accounts also reposted content from other, unrelated accounts in addition to engaging in posting and amplification behaviors. Specifically, they often reposted content about U.S. politics or NASA programs.

A number of posts from this network included content featuring a QR code; potentially as an experiment to test new mediums for Russian influence operations, the codes have evolved from loading a mobile device background image to viable links that direct users to legitimate news websites, such as the BBC and USA Today, possibly as a means of legitimizing the false content shared and amplified by these accounts. The links did not direct users to pages that reflected the content or false storyline found in the inauthentic videos. At this time, Alethea did not detect nefarious redirects or attempts that could potentially be used to gather data on users. We did not observe these assets linking to any websites—specifically clones of the websites of news outlets characteristic of Doppelgänger—directly in the text of their posts.

Amplifying Behaviors

Prior to the start of recently observed inorganic amplification relying on botnets, the accounts amplified content from other network assets using **techniques similar to those seen in Alethea's Invisible Ink report**—quote-posting other network assets' content in reply posts—**and in "Operation Overload"**—a bombardment of inquiries directed at legitimate news agencies' accounts, including the Washington Post, the BBC, France24, and Al-Jazeera, among others, requesting that the outlets verify the false information contained within the posts. For example, an account quote-posted another asset's post in response to BBC dozens of times. **Consistent with the activity set known as Matryoshka**, the accounts added text to their quote posts when replying to news outlets, such as a call to action for the outlet to review the veracity of the content in the images or videos or to explain why the outlet was "hiding" information from the public. Other posts expressed disgust or surprise about the forged images and videos. These behaviors differed from Invisible Ink posts, which seldom contained any text in the quote post.

Appendix - Mentioned News Outlets

News Outlets Linked via QR Codes:

BBC
USA Today

News Outlets Impersonated in Network Content:

AFP
al Jazeera
BBC
BFMTV
Bloomberg
Business Insider
CNN
Deutsche Welle
EuroNews
F.P. Journe
Fox News
France24
HollyWood Reporter
Japan Times
L'Équipe
Le Figaro
Le français facile avec RFI
Le Parisien
NME
Reuters
Sky News
TF1 Group
Times of Israel
USA Today
Wall Street Journal
Washington Post
Wired

ALETHEA

Alethea is a technology company that provides the market-leading solution to the Fortune 1000 and both public and private sector entities for early detection of online risks including disinformation, misinformation, stock manipulation attempts, social media manipulation, and weaponized information.

Learn more at **alethea.com**

Alethea.com