Russia leverages cyber proxies and Volga Flood assets in expansive influence efforts

A MICROSOFT THREAT INTELLIGENCE REPORT

Date: September 17, 2024

Russia and Iran have both undertaken cyber influence operations headed into the 2024 presidential election. In our third 2024 U.S. election blog published on August 8, "Iran Targeting 2024 Election," we detailed how Iranian cyber-enabled influence operations sought to undermine the Republican campaign through targeted hack-and-leak operations, covert social media personas and imposter US news sites utilizing generative AI to connect with American audiences. In this fourth US election report, Microsoft Threat Analysis Center (MTAC) observes Russia shifting its influence campaigns from denigrating President Biden to undermining the new Democratic nominee Vice President Harris.

Russian influence of US elections has remained a constant over the last decade, but in the past few months the MTAC has observed a shift in the tactics for reaching American audiences amidst a dynamic social media environment and a shifting electoral calculus. On September 4, the US government took an important step to protect against foreign influence in our upcoming election by releasing indictments[1] and sanctions[2] against Russian influence actors trying to influence the US 2024 election—including ANO Dialog, one of the Russian organizations behind the Russia-affiliated group Microsoft tracks as Ruza Flood (Doppelganger); Russia Today (RT) employees; and cyber hacktivist group RaHDit, which the government says is led by a Federal Security Service (FSB) officer and "disseminate[s] and amplif[ies] propaganda and disinformation from the Kremlin-funded and -directed organization RT."[3]

Alongside this significant U.S. government disclosure, MTAC has observed a synchronized shift by three other Russian influence operation actors, Storm-1516, Ruza Flood and Storm-1679, toward maligning the campaign of Vice President Harris. MTAC has observed, in three consecutive U.S. presidential elections, synchronized shifts by all Russian influence actors to focus on denigrating the Democratic candidate in the final 90 days before election day. MTAC assesses this synchronization on themes and messages results from top-down direction from the top of the Kremlin.

Looking ahead to Election Day, a new set of techniques—Russian cyber proxies and their amplifiers—present another, perhaps more pressing threat to the election. We expect that all Russian influence actors outlined in MTAC's previous election reports as well as this report will

[1] https://www.justice.gov/opa/pr/two-rt-employees-indicted-covertly-funding-and-directing-us-company-published-thousands, https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

[2] https://home.treasury.gov/news/press-releases/jy2559

[3] https://www.state.gov/u-s-department-of-state-takes-actions-to-counter-russian-influence-and-interference-in-u-s-elections

continue to spread divisive political content, staged videos, and even AI-enhanced propaganda ahead of the 2024 US presidential election in November.

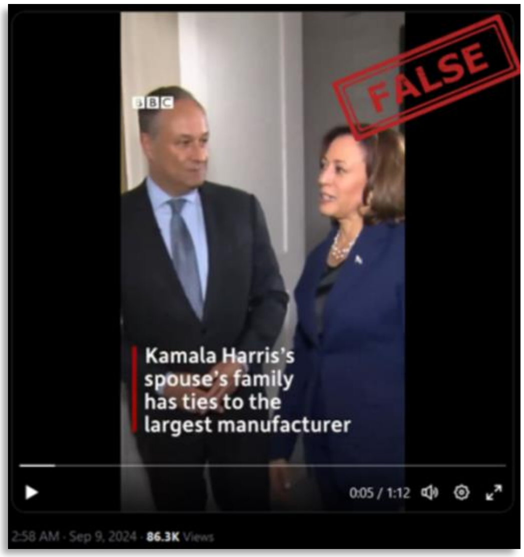
Simultaneously, based upon recent observations as reported on August 8 and MTAC's analysis of IRGC activity during the 2020 US election, we anticipate that Iranian actors will continue their activity, which may include hacking of Republican campaign targets or influence operations to incite confusion, fear, or intimidation among voters in swing states.

MTAC will produce its final, fifth election report in October detailing our findings on all of these actors as election day approaches.

Russia-affiliated influence actors Storm-1516 and Storm-1679 pivot to Harris-Walz campaign

Russian influence operations initially struggled to pivot operations aimed at the Democratic campaign following President Biden's departure from the US 2024 presidential race. In late August, however, elements of prolific Russian actor Storm-1516 began producing content implicating Vice President Harris and Governor Walz in outlandish fake conspiracy theories.

In late August and early September, Storm-1516 produced and disseminated two inauthentic videos designed to discredit Harris and stoke controversy around her campaign. The first video depicts an attack by alleged Harris supporters on what the video's amplifiers claim is a Trump rally attendee. Storm-1516 intended this video, which received millions of views, to inflame political divides by stirring racial and political tensions. The second video used an on-screen actor to fabricate false claims that Harris paralyzed a girl in a 2011 hit-and-run accident. Storm-1516, following its tried-and-true method outlined in Election Report #3, laundered this video through a website masquerading as a local San Francisco media outlet—which outlet was only created days beforehand.



Kamala Harris's spouse's family has ties to the largest manufacturer

Figure 1: A still from one of Storm-1679's videos advancing false claims about Harris.

At the beginning of September, another Russian influence actor, Storm-1679, also pivoted its influence operations to focus on Vice President Harris after primarily focusing its campaigns on France and the 2024 Paris Olympic Games for months.[4] Storm-1679 posted two videos about Harris advancing conspiracy theories and false claims about Harris's policy. One of the videos, which received more than 100,000 views on X in the four hours after its publishing on Telegram, depicted a fake New York City billboard

[4] https://blogs.microsoft.com/on-the-issues/2024/06/02/russia-cyber-bots-disinformation-2024-paris-olympics/

advancing these claims.[5] Disseminating conspiracies leveraging divisive social issues is part of Storm-1679's playbook for driving engagement with content.

These Storm-1516 and Storm-1679 operations signal a broader pivot from targeting President Biden, to targeting Vice President Harris in the final months of the election cycle. Storm-1516, adept at grabbing headlines with its outlandish fake videos and scandalous claims, and Storm-1679 will likely only escalate its targeting of the Harris-Walz campaign in the lead-up to Election Day.

Cyber proxies: One of Russia's most acute threats to the 2024 election

Russian cyber proxies and hacktivist groups disrupted Mississippi's election website and claimed to target the DNC's website during 2022's US midterm elections.[6] More recently, hacktivist group NoName057(16) claimed distributed denial-of-service (DDoS) attacks on several websites associated with the 2024 European Parliamentary Elections. Some Russian cyber proxies—like RaHDit—show overlap with activity by Russian intelligence actors, represents one of Russia's more acute threats to this November's presidential election as well.

The US government's September 4 revelation of RaHDit's ties to Russian intelligence[7] illustrates Russia's ability to use cyber proxies for effects in the information space—to leverage cyber activity to stoke fear among target audiences, sow doubt in cyber and election security, and use social media to amplify low-level attacks. RaHDit, however, while among one of Russia's more prominent cyber proxies, is not the only actor posing a threat.

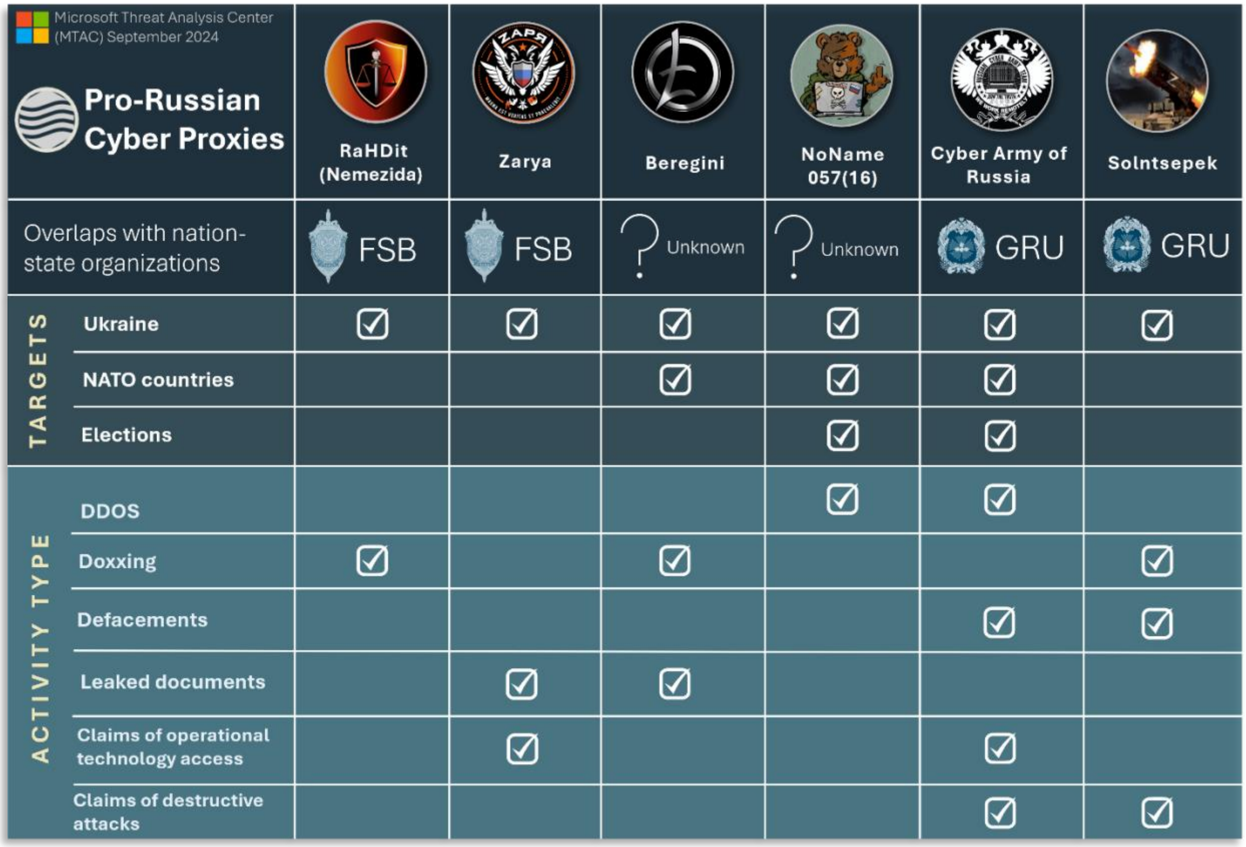
MTAC tracks several prominent Russia-affiliated cyber proxies/hacktivist groups—six of which are outlined below—that typically represent a relatively rudimentary threat in cyberspace but are capable of driving news cycles, disrupting public-facing election infrastructure, and laundering pro-Russian propaganda. Like RaHDit, several of these groups—including Solntsepek, Zarya, and Cyber Army of Russia—show overlap with Russian intelligences services.[8]

[5] t.me/Republic_Of_GaGauZia/61354

[6] usatoday.com/story/news/politics/elections/2022/11/08/2022-midterm-websites-mississippi-hit-cyber-attack/8308615001/

[7] https://www.state.gov/u-s-department-of-state-takes-actions-to-counter-russian-influence-and-interference-in-u-s-elections

[8] https://blogs.microsoft.com/on-the-issues/2023/12/07/russia-ukraine-digital-threat-celebrity-cameo-mtac/



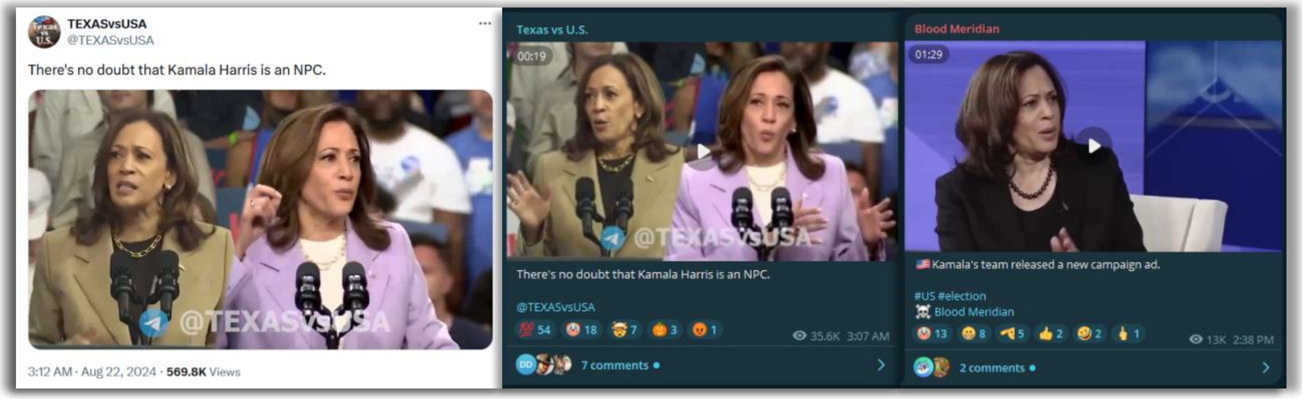
Microsoft Threat Analysis Center (MTAC) September 2024

Pro-Russian Cyber Proxies		RaHDit (Nemezida)	Zarya	Beregini	NoName 057(16)	Cyber Army of Russia	Solntsepek
Overlaps with nation-state organizations		FSB	FSB	? Unknown	? Unknown	GRU	GRU
TARGETS	Ukraine	☑	☑	☑	☑	☑	☑
	NATO countries			☑	☑	☑	
	Elections				☑	☑	
ACTIVITY TYPE	DDOS				☑	☑	
	Doxxing	☑		☑			☑
	Defacements					☑	☑
	Leaked documents		☑	☑			
	Claims of operational technology access		☑			☑	
	Claims of destructive attacks					☑	☑

For Russia, cyber proxies offer a method for potentially laundering compromising information garnered from a hack-and-leak operation while maintaining a veil of plausible deniability for the Kremlin. Cyber proxies may also be employed for stoking fear of electoral disruption just before or on Election Day in November. To avoid counterproductive amplification, media, policymakers, and defenders of election infrastructure should be wary of overinflating the threat of these groups in the public forum yet should remain vigilant of their activity related to the election.

Russia-affiliated influence actor Volga Flood (Storm-1841, aka Rybar) collaborates with cyber proxies

Volga Flood (formerly Storm-1841, or Rybar) brands itself as a grassroots military blogger—in reality, however, it is a media propaganda enterprise focusing on a diverse catalogue of activity sets.



TEXASvsUSA
@TEXASvsUSA

There's no doubt that Kamala Harris is an NPC.

3:12 AM · Aug 22, 2024 · **569.8K** Views

Texas vs U.S.

There's no doubt that Kamala Harris is an NPC.

@TEXASvsUSA

💯 54 🤡 18 🤯 7 🎃 3 😡 1 👁 35.6K 3:07 AM

7 comments

Blood Meridian

🇺🇸 Kamala's team released a new campaign ad.

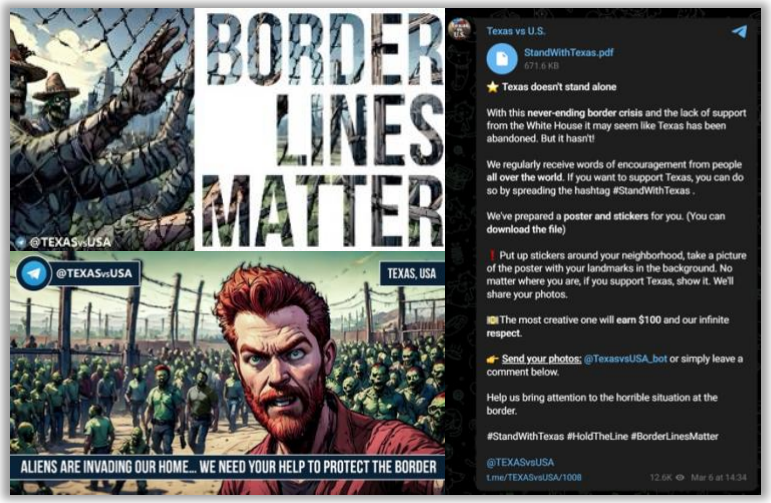
#US #election
☠️ Blood Meridian

🤡 13 😁 8 🤏 5 👍 2 🤣 2 🖕 1 👁 13K 2:38 PM

2 comments

Figure 2: Volga Flood posts focused on Harris.

As we reported in our August 2024 election report, Volga Flood continues to operate covert social media channels that target US audiences. Volga Flood amplifies allegedly hacked-and-leaked materials from cyber proxies like Beregini and RaHDit. Volga Flood also posts fake investigations on its social media channels which at times use insights supposedly derived from the allegedly hacked and leaked materials from those cyber proxies.



BORDER LINES MATTER
@TEXASvsUSA
@TEXASvsUSA
TEXAS, USA
ALIENS ARE INVADING OUR HOME... WE NEED YOUR HELP TO PROTECT THE BORDER

Texas vs U.S.

StandWithTexas.pdf
671.6 KB

⭐ Texas doesn't stand alone

With this **never-ending border crisis** and the lack of support from the White House it may seem like Texas has been abandoned. But it hasn't!

We regularly receive words of encouragement from people **all over the world**. If you want to support Texas, you can do so by spreading the hashtag #StandWithTexas .

We've prepared a **poster and stickers** for you. (You can **download the file**)

❗ Put up stickers around your neighborhood, take a picture of the poster with your landmarks in the background. No matter where you are, if you support Texas, show it. We'll share your photos.

💵 The most creative one will **earn $100** and our infinite **respect**.

👉 Send your photos: @TexasvsUSA_bot or simply leave a comment below.

Help us bring attention to the horrible situation at the border.

#StandWithTexas #HoldTheLine #BorderLinesMatter

@TEXASvsUSA
t.me/TEXASvsUSA/1008 12.6K 👁 Mar 6 at 14:34

Figure 3: Volga Flood content focused on the Southern border from its US-focused channel.

In 2023 hacktivist group Beregini claimed to compromise Kazakhstan's Main Intelligence Directorate and arms company Kazspetsexport. Volga Flood used the documents from Beregini's alleged hack to claim that the Kazakh government funneled weapons to Ukraine through the British government.

Volga Flood's leadership—which includes EU-sanctioned Mikhail Zvinchuk[9]—consists of former employees of the Russian Ministry of Defense and the late Yevgeny Prigozhin's Patriot Media Group. Volga Flood has previously worked for Russian

[9] https://gels-avoirs.dgtresor.gouv.fr/Gels/RegistreDetail?idRegistre=6742

state corporation Rostec and, MTAC assesses, receives some of its resourcing from the Russian Presidential Administration. Volga Flood is among the leading Russian actors leveraging AI to scale its operations beyond the capabilities of its teams that include regional analytics, illustration, mapping, and foreign language expertise.

Volga Flood's eye-catching visuals target young audiences, both domestically and internationally, through the illusion of a grassroots, crowdfunded organization obscuring connections to the Russian government. Volga Flood's capabilities are further illustrated by its ability to leverage connections across Central Asia and the Middle East to broaden Kremlin cooperation in media and education. Volga Flood's ability to respond to breaking news events through its covert channels—such as the recent Southport riots in the UK—demonstrate its versatility and nimbleness. Volga Flood is forward-thinking and has shown the ability to adapt quickly to shifting US political discussion, a capability that should be closely monitored during breaking news events related to the 2024 US presidential election.[10]

Ruza Flood's connections to Russian state organization ANO Dialog

Ruza Flood hopes that stoking social rifts among US and European audiences will produce anti-Ukraine sentiments. Recent disclosures by the US Department of Justice in early September highlight Ruza Flood's backing by the Russian government's Presidential Administration and the role in Ruza Flood activity of state organization ANO Dialog. These disclosures confirm historic connections observed by Microsoft. ANO Dialog employees created two of the Ruza Flood covert propaganda outlets within two weeks after Russia's full-scale invasion of Ukraine, which were later operated by teams of foreigners and young, multilingual Russians. We assess that these teams almost certainly work at the direction of Dialog and disseminate propaganda preferred by the Russian Presidential Administration.

Public revelations and sanctions have forced Ruza Flood to shift some of its cyber influence infrastructure. **In the days following the US government's seizures of Ruza Flood's web domains, we observed this actor moving media outlets from seized domains to new ones, where content can again be readily accessed**.

China's Storm-1852 shows increased reach before disruption

A Chinese-linked influence actor Microsoft tracks as Storm-1852 successfully pivoted to short-form video content that criticizes the Biden administration and Harris campaign before some of its assets disappeared from social media following reports of its activity. While most Storm-1852 personas masquerade as conservative US voters voting for Trump, a handful of accounts also create anti-Trump content and use political slogans and hashtags associated

[10] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf

with American progressive politics. Storm-1852 personas respond quickly to political events—much more nimbly and effectively than China-linked actor Taizi Flood, which relies on massive cross-platform campaigns. Instead, Storm-1852 prioritizes cultivating an audience by reposting content, replying to comments, polling users, and organizing "follow trains."[11] This hands-on, interactive approach makes this actor more agile in influencing public conversations. Directly after the first attempted assassination of former President Trump, Storm-1852 accounts began live re-posting content from influencers and commentators alleging Democrats' involvement and released original short-form videos edited from news footage four to five hours later. Still, Storm-1852 operators do not appear interested in supporting a particular candidate—rather, they likely intend to seed doubt and confusion among American voters ahead of the 2024 presidential election.

MTAC will continue to monitor foreign influence activity up to and through Election Day in November and we plan to have a final pre-election update available in mid-October 2024.

[11] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC-East-Asia-Report.pdf