OPERATION OVERLOAD

Activity Update - September 2024

CHECK FIRST

Reset·Tech

Operation Overload

Activity Update September 2024

Version	Date	Description
1	12 Sept 2024	Initial release

This update report intends to cover the evolutions we observed in the outputs and techniques used by the actors behind “Operation Overload” since our report published in June 2024[1].

The initial report on "Operation Overload" details a significant, ongoing disinformation campaign that primarily targets fact-checkers, newsrooms, and researchers across the globe. The operation seeks to inundate its targets with false information and manipulated content, particularly narratives that support Kremlin interests, such as anti-Ukraine propaganda.

Central to the campaign is a coordinated effort involving the mass distribution of emails to fact-checkers and journalists, directing them to false news stories promoted by anonymous X (formerly Twitter) accounts, pro-Russian Telegram channels or websites. The disseminated content is varied and includes videos falsely bearing legitimate media logos, doctored images of graffiti, and fabricated social media posts, all designed to create and amplify misleading narratives.

Notably, we can now link the operation directly to Russia thanks to newly accessed information.

The email campaign targeting fact-checkers and journalists has shown both consistency in operational tactics and adaptability in content focus. The volume of emails has been significantly increasing in the last three months — particularly during global events — with a distinct focus on the 2024 Paris Olympics, where the operation sought to exploit public interest and concern.

We have gained access to a new dataset of targeted organisations, which we have cross-referenced with our own data and successfully verified its reliability. This dataset has provided us with a clearer understanding of the scope and origins of the operation, revealing a broader targeting range than initially identified.

[1] Operation Overload: how pro-Russian actors flood newsrooms with fake content and seek to divert their efforts - CheckFirst - https://checkfirst.network/operation-overload-how-pro-russian-actors-flood-newsrooms-with-fake-content-and-seek-to-divert-their-efforts/

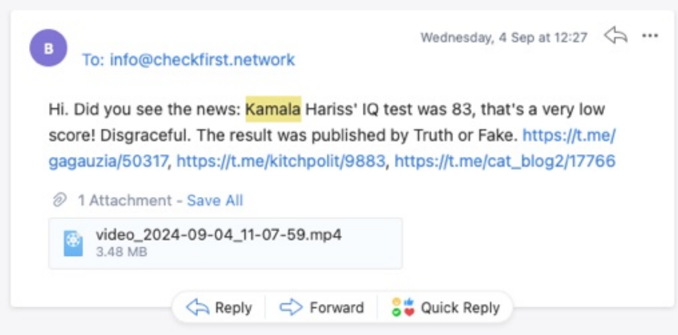
Narrative Focus and Tactical Shifts

Emails sent in between January 1 and September 12024 were analysed. The contents of the messages reflect a clear alignment with global events. For example, during the Paris Olympics the operation focused heavily on narratives related to the security and safety of the event. False claims about terrorist threats, public health and safety issues, and misinformation regarding the French government's handling of the Games were widely spread.

The operation focused heavily on the "OLYMPICS HAS FALLEN" narrative[2], a series of false documentaries using AI-generated content. This campaign is particularly sophisticated due to the involvement of advanced techniques such as voice cloning of well-known public figures (e.g. Elon Musk) to lend credibility to the false information being disseminated. This period also marked the highest intensity of email activity within the analysed time frame, indicating dedicated efforts and resources to influence journalistic and mediatic perceptions during a major international event. Furthermore, over 50% of the content linked to the operation and posted on Telegram between June and August 2024 promoted narratives portraying the Olympic Games as a catastrophic, disruptive, or generally worthless event.

Beyond the Olympics, the operation continued to propagate disinformation about the economic situation in France. These emails often exaggerated or entirely fabricated crises, aiming to undermine public trust in the country's economic stability. Additionally, disinformation related to the Russian-Ukrainian conflict persisted, using false accusations of corporate support to the war effort to attempt to tarnish the reputation of well known Western companies. Anti-Ukrainian narratives were also prevalent, such as the portrayal of Ukrainian refugees living in the West as dangerous or somewhat stupid people.

The evolution of these narratives over time highlights the continuation of a clear pattern: the operation actively adapts its content to align with high-profile events and areas of public interest. Initially centred on broader geopolitical disinformation, the focus shifted to event-driven narratives as the Olympics approached, demonstrating the operation's responsiveness to global events. An analysis of the most recent emails and content pieces shows that it now appears to be pivoting towards its next big target: the U.S. presidential elections in November.



B

To: info@checkfirst.network

Wednesday, 4 Sep at 12:27

Hi. Did you see the news: Kamala Hariss' IQ test was 83, that's a very low score! Disgraceful. The result was published by Truth or Fake. https://t.me/gagauzia/50317, https://t.me/kitchpolit/9883, https://t.me/cat_blog2/17766

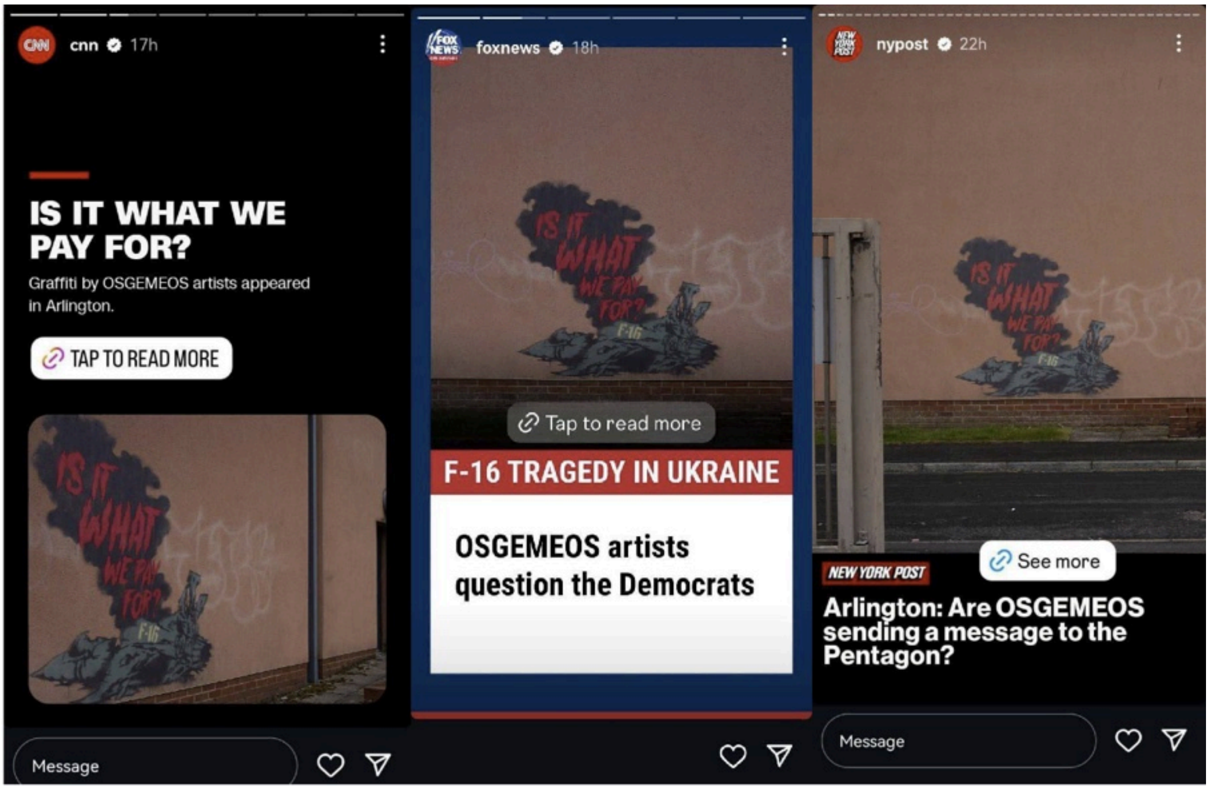
1 Attachment - Save All

video_2024-09-04_11-07-59.mp4
3.48 MB

Fig. 1: Overload email received Sep 4 2024 accusing Kamala Hariss of having a low IQ

[2] How Russia is trying to disrupt the 2024 Paris Olympic Games - Microsoft - https://blogs.microsoft.com/on-the-issues/2024/06/02/russia-cyber-bots-disinformation-2024-paris-olympics/

Starting at the end of August 2024, emails containing narratives seemingly targeted at U.S. audiences were sent out. We counted 22 pieces of content related to the upcoming U.S. elections. These either use forgeries of U.S. media brand content (such as Fox News), or use pictures and names of U.S. officials to support their false claims. The first week of September saw an increase in the volume of emails related to U.S. politics. Some narratives are clearly attempting to harm the Harris campaign, attempting for example to spread rumours about the Democrats' candidate low IQ level (Fig. 1).



IS IT WHAT WE PAY FOR?

Graffiti by OSGEMEOS artists appeared in Arlington.

F-16 TRAGEDY IN UKRAINE

OSGEMEOS artists question the Democrats

NEW YORK POST

Arlington: Are OSGEMEOS sending a message to the Pentagon?

Fig. 2: Screenshots of fake Instagram Stories allegedly posted by the Instagram accounts of US media outlets, crediting the artist OSGEMEOS[3] for a graffiti depicting a crashed F16 with the caption, "Is this what we pay for?".

Another striking example of both this shift of narratives towards a U.S. audience and the ability of operatives to create relatively quickly fake content is the following example of the exploitation of the crash of an US donated F16 fighter jet in Ukraine. The crash occurred on August 26. On September 2, an email containing a doctored photo of graffiti featuring a smoking F-16 aircraft was sent to targets, including several false Instagram screenshots from the U.S. media Fox News, The New York Post and CNN (Fig 2).

[3] OSGEMEOS - Wikipedia - https://en.wikipedia.org/wiki/OSGEMEOS

New formats for content amalgamation

We discovered two new types of content in addition to the ones we knew from our initial report: the most prolific Russian-language Telegram channels associated with Operation Overload started publishing the format of fake TikTok videos impersonating the TikTok accounts of media outlets and other organisations. The other format involved screenshots of manipulated covers of reputable newspapers or magazines containing articles that had never been published by the outlets. This trend for ever-evolving content diversification is aimed to amplify the effects of content amalgamation, a key strategy we emphasised in our initial report on Overload. The tactic is designed to blend false information across different content formats, thereby effectively enhancing the believability of the narratives.

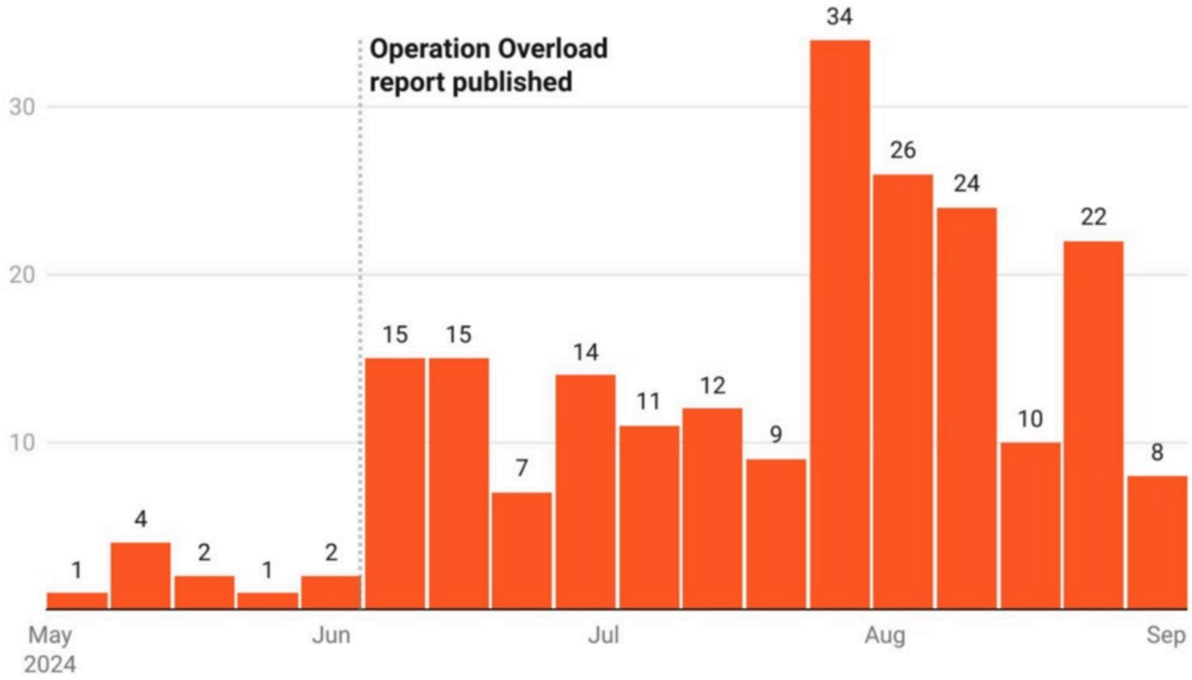
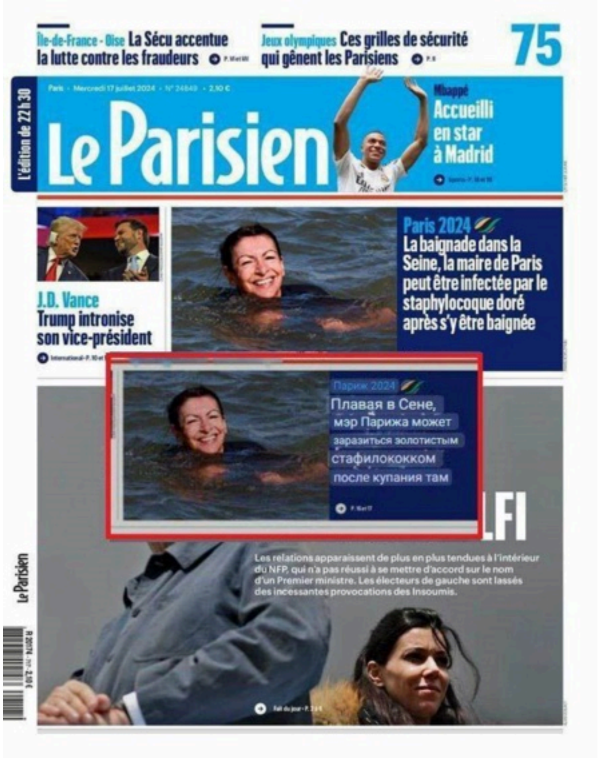


Fig. 3: The chart shows the surge of activity of the two main Telegram channels linked to the Kremlin-backed Operation Overload, @belshvarka and @thehandofthekremlin. The weekly content production saw exponential growth between June and August, with a median of five new pieces posted per day by the analysed channels during this period.



Île-de-France - Oise La Sécu accentue la lutte contre les fraudeurs

Jeux olympiques Ces grilles de sécurité qui gênent les Parisiens

75

L'édition de 22 h 30

Paris · Mercredi 17 juillet 2024 · N° 24849 · 2,10 €

Le Parisien

Mbappé Accueilli en star à Madrid

J.D. Vance Trump intronise son vice-président

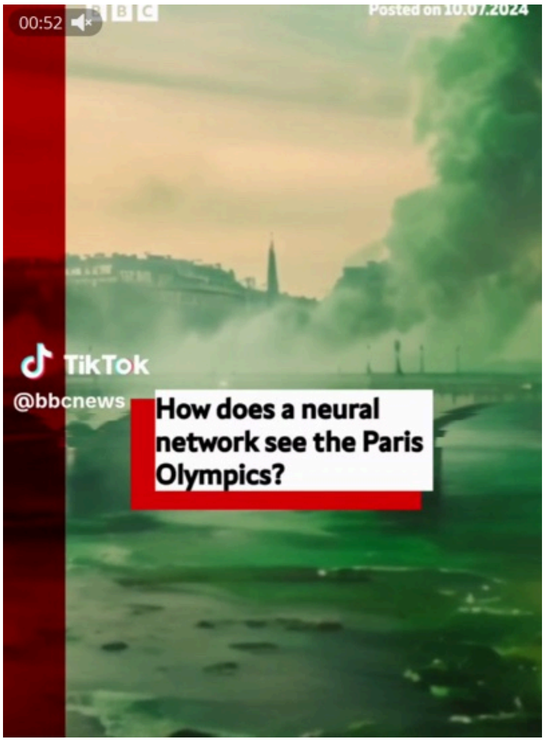
Paris 2024 La baignade dans la Seine, la maire de Paris peut être infectée par le staphylocoque doré après s'y être baignée

Париж 2024 Плавая в Сене, мэр Парижа может заразиться золотистым стафилококком после купания там

LFI

Les relations apparaissent de plus en plus tendues à l'intérieur du NFP, qui n'a pas réussi à se mettre d'accord sur le nom d'un Premier ministre. Les électeurs de gauche sont lassés des incessantes provocations des Insoumis.

Le Parisien



00:52

BBC

Posted on 10.07.2024

TikTok

@bbcnews

How does a neural network see the Paris Olympics?

Fig. 4: New content formats boost the effects of content amalgamation: a fake cover of the French newspaper Le Parisien, featuring an imaginary story about the mayor of Paris contracting a Staphylococcal infection after swimming in the Seine during the Olympic Games; a fake TikTok video allegedly posted by the TikTok account of BBC, @bbcnews, showcasing a chaotic portrayal of the Olympic Games generated by a neural network.

Targeting of Contacts

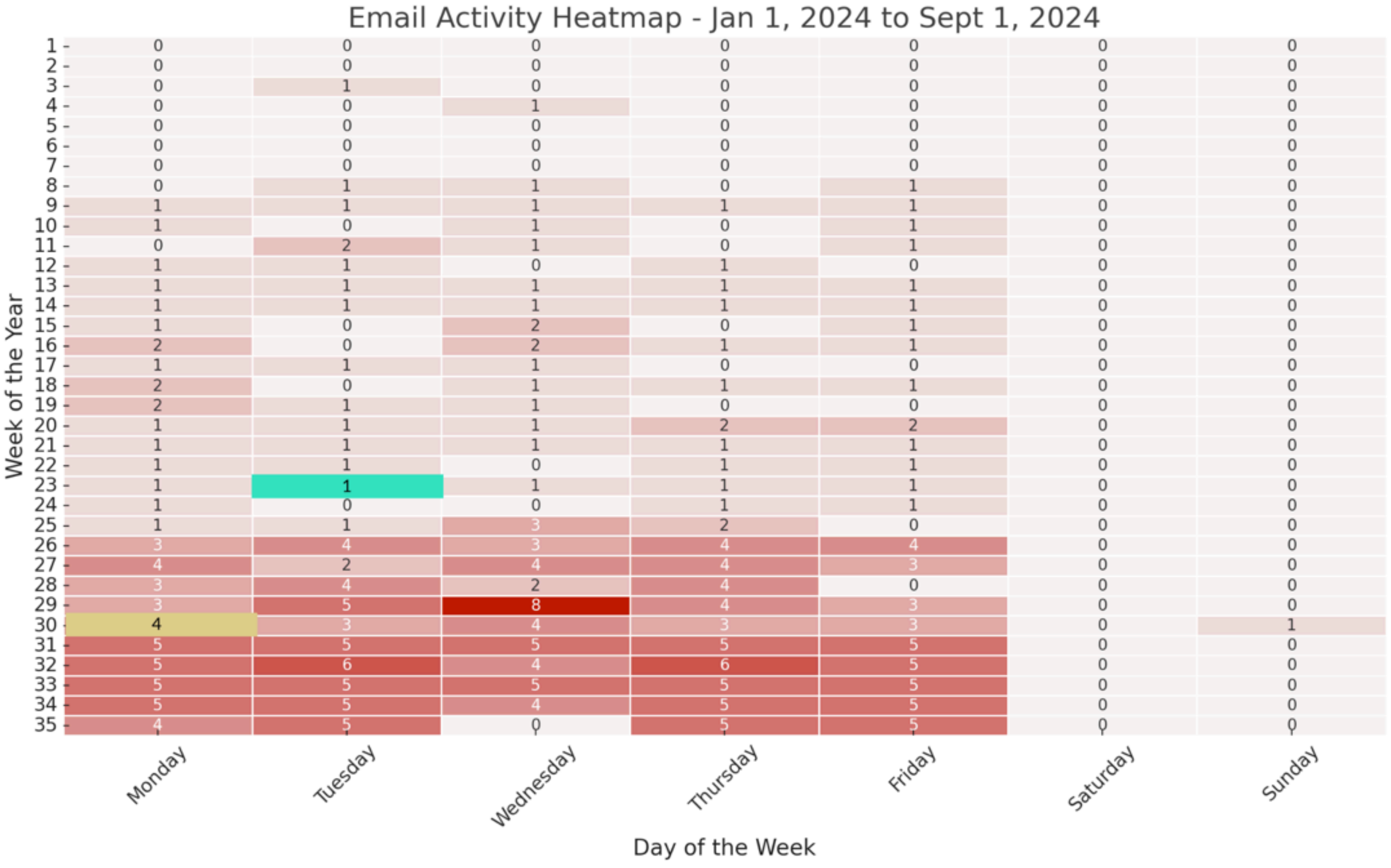
While our original report stated that at least 20 organisations were targeted by email, recent findings have provided us with a clearer view of how the operation targets its recipients. An analysis of a contact list CheckFirst could access — and proved by cross-referencing to be used by the operatives — reveals that a total of 245 email addresses belonging to researchers, media and fact-checking organisations have been used by the operatives.

Approximately 11% of these email addresses are nominative, which suggests a focused effort to directly reach individuals within the targeted organisations. The remaining 89% are more generic addresses, such as contact@media.com, likely intended for broader distribution within the targeted organisations. The nature of these emails, combined with the inclusion of generic addresses, reflects the operation's dual strategy: to penetrate organisations at an individual level while also aiming for widespread dissemination of disinformation. The operation appears to aim at a wide range of media outlets and fact-checking organisations across different regions, with a significant focus on French media. Some of the most frequently targeted organisations include major French news outlets such as *Centre France*, *La Dépêche*, *20 Minutes*, or *TF1*. Additionally, international media giants like *NBC Universal*, *Turner Broadcasting*, or *The Wall Street Journal* are also on the target list[4]. This distribution suggests that the operation is not confined to one region but is instead a coordinated effort to influence media coverage and public perception across multiple countries and continents.

[4] See Annex 1

Email Volume

The heatmap of email activity from January to September 2024, provides a comprehensive view of the operation's intensity over time. Throughout this period, an estimated total[5] of 71,000 emails were sent, providing us an idea of how extensive the scale of the operation is. The most significant periods of email activity coincide with major global events, underscoring the operation's strategic timing. For instance, there was a considerable surge in email activity during the Paris Olympics, especially from late July to early August. This period saw an increase in coordinated disinformation attempts, with daily email volumes often surpassing the typical levels observed earlier in the year.



Week of the Year	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	1	0	0	0	0	0
4	0	0	1	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	1	1	0	1	0	0
9	1	1	1	1	1	0	0
10	1	0	1	0	1	0	0
11	0	2	1	0	1	0	0
12	1	1	0	1	0	0	0
13	1	1	1	1	1	0	0
14	1	1	1	1	1	0	0
15	1	0	2	0	1	0	0
16	2	0	2	1	1	0	0
17	1	1	1	0	0	0	0
18	2	0	1	1	1	0	0
19	2	1	1	0	0	0	0
20	1	1	1	2	2	0	0
21	1	1	1	1	1	0	0
22	1	1	0	1	1	0	0
23	1	1	1	1	1	0	0
24	1	0	0	1	1	0	0
25	1	1	3	2	0	0	0
26	3	4	3	4	4	0	0
27	4	2	4	4	3	0	0
28	3	4	2	4	0	0	0
29	3	5	8	4	3	0	0
30	4	3	4	3	3	0	1
31	5	5	5	5	5	0	0
32	5	6	4	6	5	0	0
33	5	5	5	5	5	0	0
34	5	5	4	5	5	0	0
35	4	5	0	5	5	0	0

🟩	🟨
Publication of the Overload report	PARIS 2024

[5] Estimation reached by multiplying the total amount of emails Check First has received by the number of contacts found in the dataset we could access.

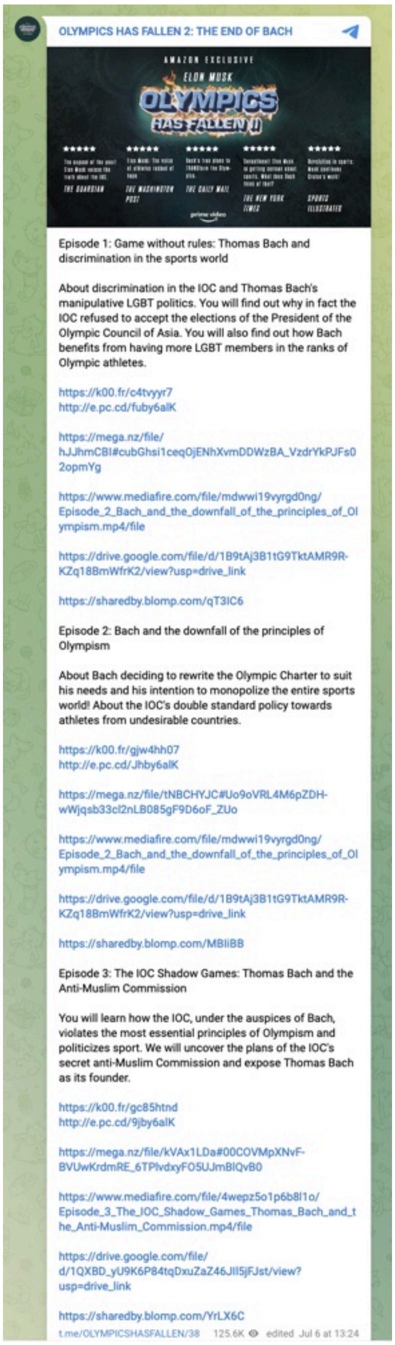
Use of Telegram Channels

The examination of the emails reveals that nearly every email includes one or more links to Telegram channels. This indicates that Telegram is a central hub for the operation's activities. The platform's appeal lies in its ability to host large chat groups where information — accurate or otherwise — can be quickly disseminated to a wide audience, notably through the email campaign.

The reliance on Telegram is likely strategic, leveraging the platform's features to amplify disinformation campaigns, as demonstrated in our first report. For instance, during the "OLYMPICS HAS FALLEN" campaign, emails directed recipients to a specific Telegram channel where the narrative was being further propagated, often with added layers of misinformation or de-contextualisation meant to deceive or cause confusion.

We analysed the activity of the two most active Russian-language channels behind the operation, *@belshvarka* and *@thehandofthekremlin*, and found that more than 200 content pieces were posted between June and August 2024[6]. The hallmark format associated with Overload – fake videos impersonating the logos of actual media outlets – accounts for 50% of the analysed content. Additionally, the three content types already identified in our first report — fake Instagram Stories, doctored graffiti photos, and fabricated articles mimicking the websites of media outlets — account for approximately 30% of the content.

More generally, the Telegram channels linked in the emails often cover common topics — anti-Western rhetoric, conspiracy theories, and narratives aimed at eroding public trust in institutions. By directing the email recipients to these channels, the operation aims to both obtain a broader audience and engage users in an ecosystem of disinformation, while exposing them to a steady stream of content that reinforces the campaign's narratives.



OLYMPICS HAS FALLEN 2: THE END OF BACH

Episode 1: Game without rules: Thomas Bach and discrimination in the sports world

About discrimination in the IOC and Thomas Bach's manipulative LGBT politics. You will find out why in fact the IOC refused to accept the elections of the President of the Olympic Council of Asia. You will also find out how Bach benefits from having more LGBT members in the ranks of Olympic athletes.

https://k00.fr/c4tvyyr7
http://e.pc.cd/fuby6alK

https://mega.nz/file/hJJhmCBI#cubGhsi1ceqOjENhXvmDDWzBA_VzdrYkPJFs02opmYg

https://www.mediafire.com/file/mdwwi19vyrgd0ng/Episode_2_Bach_and_the_downfall_of_the_principles_of_Olympism.mp4/file

https://drive.google.com/file/d/1B9tAj3B1tG9TktAMR9R-KZq18BmWfrK2/view?usp=drive_link

https://sharedby.blomp.com/qT3IC6

Episode 2: Bach and the downfall of the principles of Olympism

About Bach deciding to rewrite the Olympic Charter to suit his needs and his intention to monopolize the entire sports world! About the IOC's double standard policy towards athletes from undesirable countries.

https://k00.fr/gjw4hh07
http://e.pc.cd/Jhby6alK

https://mega.nz/file/tNBCHYJC#Uo9oVRL4M6pZDH-wWjqsb33cl2nLB085gF9D6oF_ZUo

https://www.mediafire.com/file/mdwwi19vyrgd0ng/Episode_2_Bach_and_the_downfall_of_the_principles_of_Olympism.mp4/file

https://drive.google.com/file/d/1B9tAj3B1tG9TktAMR9R-KZq18BmWfrK2/view?usp=drive_link

https://sharedby.blomp.com/MBIiBB

Episode 3: The IOC Shadow Games: Thomas Bach and the Anti-Muslim Commission

You will learn how the IOC, under the auspices of Bach, violates the most essential principles of Olympism and politicizes sport. We will uncover the plans of the IOC's secret anti-Muslim Commission and expose Thomas Bach as its founder.

https://k00.fr/gc85htnd
http://e.pc.cd/9jby6alK

https://mega.nz/file/kVAx1LDa#00COVMpXNvF-BVUwKrdmRE_6TPlvdxyFO5UJmBIQvB0

https://www.mediafire.com/file/4wepz5o1p6b8l1o/Episode_3_The_IOC_Shadow_Games_Thomas_Bach_and_the_Anti-Muslim_Commission.mp4/file

https://drive.google.com/file/d/1QXBD_yU9K6P84tqDxuZaZ46JIl5jFJst/view?usp=drive_link

https://sharedby.blomp.com/YrLX6C

t.me/OLYMPICSHASFALLEN/38 125.6K edited Jul 6 at 13:24

[6] Note that the analysis focuses only on the number of produced content on Telegram. We did not follow the amplification of the content on X (formerly Twitter) by the network of inauthentic accounts, which we identified as pingers/seeders in our June report.

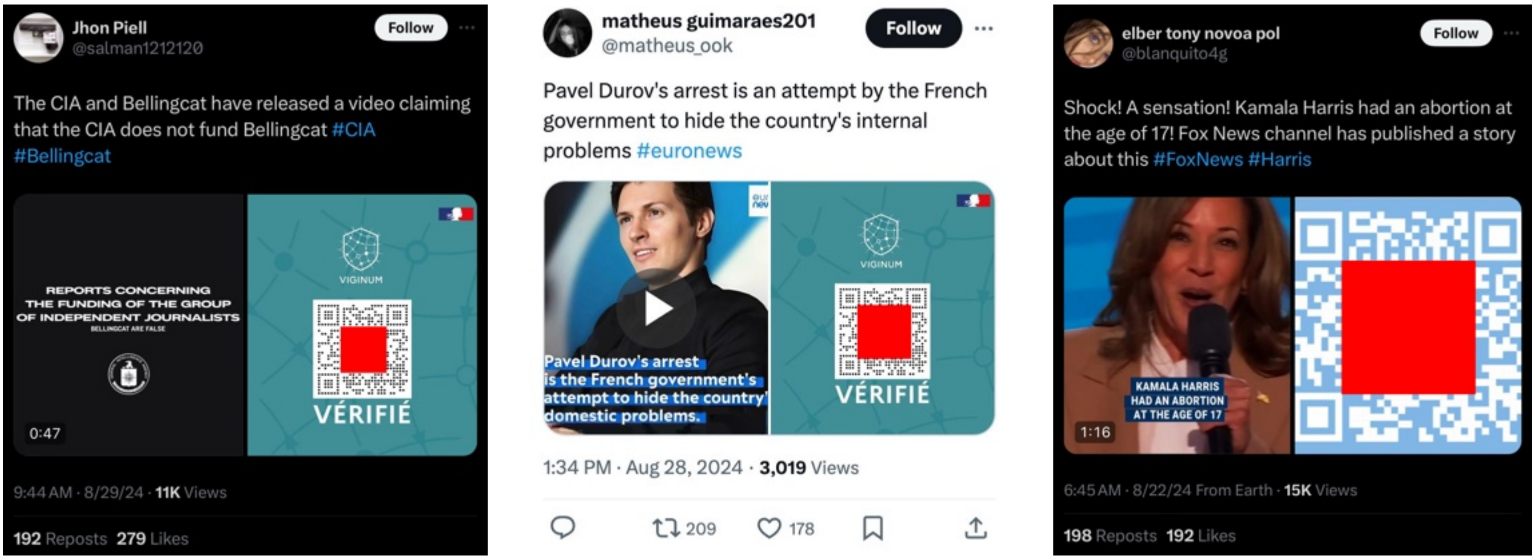
Fig. 5: Screenshot of the post promoting the episodes of "Olympics has fallen" on Telegram

Continued Use of QR Codes in Disinformation

A notable technique that was highlighted in the original report — the use of QR codes — has continued to play a significant role in or alongside the dissemination of disinformation. Recent examples on X (formerly Twitter) demonstrate how QR codes are being employed in increasingly sophisticated ways. Specifically, the new QR codes initially direct users to a landing page on "me-qr.com," a service which offers free dynamic QR code creation. The landing page itself is cluttered with ads, which can be misleading, but what is more surprising is that after navigating through this page, users are then redirected to the website of the French government agency VIGINUM, a legitimate entity responsible for protection against online interference by foreign state actors.

The QR codes are branded with VIGINUM's visual identity, showing a clear intent to impersonate the agency in an attempt to add an "official" seal of credibility to the associated piece of disinformation. However, the reason why users are redirected to VIGINUM's page remains unclear.

Moreover, it remains important to note that the links embedded within these QR codes can be changed at any time. This means that while the current destination leads to a legitimate website, these links could easily be redirected to malicious websites in the future, thereby further complicating the ability to track and mitigate the impact of these disinformation campaigns and posing a security risk for users. The dynamic nature of these QR codes makes them a particularly dangerous tool in the arsenal of those orchestrating Operation Overload.


Jhon Piell
@salman1212120
Follow

The CIA and Bellingcat have released a video claiming that the CIA does not fund Bellingcat #CIA #Bellingcat

REPORTS CONCERNING THE FUNDING OF THE GROUP OF INDEPENDENT JOURNALISTS
BELLINGCAT ARE FALSE
0:47
VIGINUM
VÉRIFIÉ

9:44 AM · 8/29/24 · 11K Views

192 Reposts 279 Likes

matheus guimaraes201
@matheus_ook
Follow

Pavel Durov's arrest is an attempt by the French government to hide the country's internal problems #euronews

Pavel Durov's arrest is the French government's attempt to hide the country's domestic problems.
VIGINUM
VÉRIFIÉ

1:34 PM · Aug 28, 2024 · 3,019 Views

209 178

elber tony novoa pol
@blanquito4g
Follow

Shock! A sensation! Kamala Harris had an abortion at the age of 17! Fox News channel has published a story about this #FoxNews #Harris

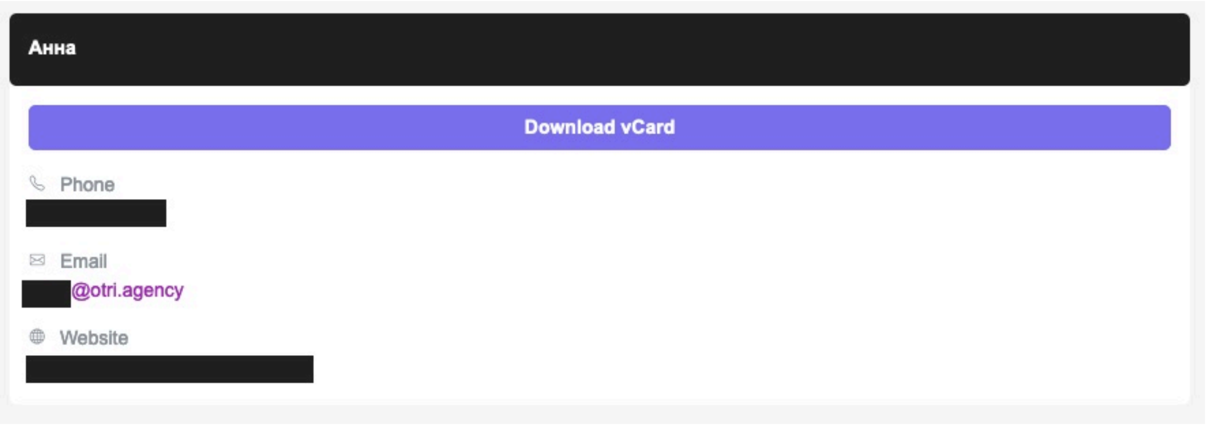
6:45 AM · 8/22/24 From Earth · 15K Views

198 Reposts 192 Likes

Fig 6: QR codes amplified by inauthentic X accounts

The Russian Connection

Further investigation into Overload’s QR codes suggests that they were likely created as early as 2022 by an individual connected to Otri, a Russian "full-cycle marketing agency." Otri[7] specialises in developing and implementing marketing strategies, especially through digital communication channels. This finding is consistent with the observations in our initial Operation Overload report , where we noticed that one of the emails had been written in Russian, indicating a Russian origin of the operation.



Анна

Phone
[redacted]

Email
[redacted]@otri.agency

Website
[redacted]

Fig. 7: vCard of an employee of Otri attached to the account where the QR Code is hosted

In addition to this evidence, the dataset we recently gained access to confirms that one of the accounts used to send emails in August 2024 was accessed from a residential Russian IP address at the time the emails were sent. This information further confirms that Operation Overload is likely originating from Russia, reinforcing our initial findings, attributing the action to operatives based in Russia, pushing Kremlin-aligned political objectives.

[7] ИП Усманов Шохрух Бахтиёрович - RusProfile - https://www.rusprofile.ru/ip/318385000026569

Conclusion

Operation Overload is a clear example of coordinated inauthentic behaviour designed to manipulate public perception. With over 71,000 emails received to a carefully curated list of contacts, the operation has used sophisticated tactics, including dynamic QR codes, anonymous inauthentic accounts on X (formerly Twitter), Telegram channels and a network of fake media websites, to spread disinformation. The surge in activity during the Paris 2024 Olympics highlights the operation's strategic timing, aiming at exploiting global events for maximum impact.

While sending emails is not illegal, the methods used in this campaign violate the Terms of Service of platforms such as Gmail, which prohibit activities such as spamming, phishing, and creating misleading content[8]. The operation's abuse of these services underscores the need for stronger enforcement of digital platform policies to prevent such malicious usage.

Moreover, there are clear indications that Operation Overload is shifting its focus toward the upcoming U.S. elections, with emerging narratives tailored to influence this significant event. This evolution in the operation's strategy highlights the ongoing threat posed by such disinformation campaigns, making vigilance and proactive measures more critical than ever.

[8] GOOGLE TERMS OF SERVICE Effective May 22, 2024
https://www.gstatic.com/policies/terms/pdf/20240522/ks8shls0/google_terms_of_service_en_eu.pdf

Annexes

1. Targeted organisations

15min.lt	20minut.fr	20minutes.fr	211check.org
404media.co	aap.com.au	afghanfact.com	africacheck.org
aljazeera.net	altnews.in	aosfatos.org	apa.at
barrons.com	bbc.co.uk	bbc.com	beamreports.com
bellingcat.com	blackdotresearch.sg	bloomberg.net	boliviaverifica.bo
boomlive.in	bufale.net	butac.it	centrefrance.com
checkfirst.network	checkyourfact.com	cheddar.com	civilnet.am
colombiacheck.com	congocheck.net	correctiv.org	dailymail.com
debunk.org	delfi.ee	delfi.lt	delfi.lv
demagog.cz	demagog.org.pl	denver7.com	denverpost.com
detector.media	diez.md	digiteye.in	dn.se
dogrula.org	dogrulukpayi.com	domain.com	dpa.com
dubawa.org	dw.com	ecuadorchequea.com	efcsn.com
efe.com	estadao.com	euronews.com	facta.news
factcheck.ge	factcheck.org	factcheck.vlaanderen	factcheckhub.com
factcheckni.org	factcheckzw.org	factcrescendo.com	factly.in
factnameh.com	factuel.media	factwatch.org	faktabaari.fi
faktisk.no	faktograf.hr	faktoje.al	fastcheck.cl
fatabyyano.net	firstcheck.in	focus-money.de	focus.de
foxnews.com	france24.com	francemm.com	fullfact.org
fundacionperiodismo.org	gannett.com	ghanafact.com	gmail.com
gwaramedia.com	hibrid.info	hkbu.edu.hk	hku.hk
huffingtonpost.fr	hurriyet.com.tr	i-pmr.com	info-prim.md

info-veritas.com	infotag.md	institutsgi.sk	intoday.com
istinomer.rs	jpost.com	jtbc.co.kr	jurnaltv.md
kallkritikbyran.se	kallxo.com	kly.id	krik.rs
ksjfactcheck.org	ladepeche.fr	ladepechenews.com	lakmusz.hu
lallantop.com	lavoce.info	leadstories.com	lefigaro.fr
lemonde.fr	lepoint.fr	lesechos.fr	lesechosleparisien.fr
lessurligneurs.eu	lexpress.fr	liberation.fr	mdfgeorgia.ge
mediapart.fr	mfcc.mn	mfwa.org	milliyet.com.tr
misbar.com	mygopen.com	nbcuni.com	newschecker.in
newsmeter.in	newsmobile.in	newtral.es	noi.md
nypost.com	nytimes.com	observador.pt	observer.co.uk
open.online	ostro.si	outlook.com	pa.media
pagellapolitica.it	pbs.org	point.md	poligrafo.pt
politico.com	poynter.org	pravda.org.pl	probe.ph
protv.md	pti.in	publico.pt	radiofrance.com
rebaltica.com	rfi.fr	rmit.edu.au	rnbo.gov.ua
sciencepresse.qc.ca	spiegel.de	stiri.md	stopfals.md
suara.com	sueddeutsche.de	telegraph.co.uk	teyit.org
tf1.fr	tfc-taiwan.org	the-sun.co.uk	theconversation.edu.au
theguardian.com	thejournal.ie	thequint.com	thip.in
thomsonreuters.com	time.com	tirto.id	tjekdet.dk
turner.com	tvazteca.com	unghiul.com	unimedia.md
uol.com.br	verafiles.org	verificat.cat	veriteresearch.org
vesti.md	viralcheck.pt	vishvasnews.com	volksverpetzer.de
vrt.be	washpost.com	welt.de	wsj.com
zastone.ba	zddk.eu		