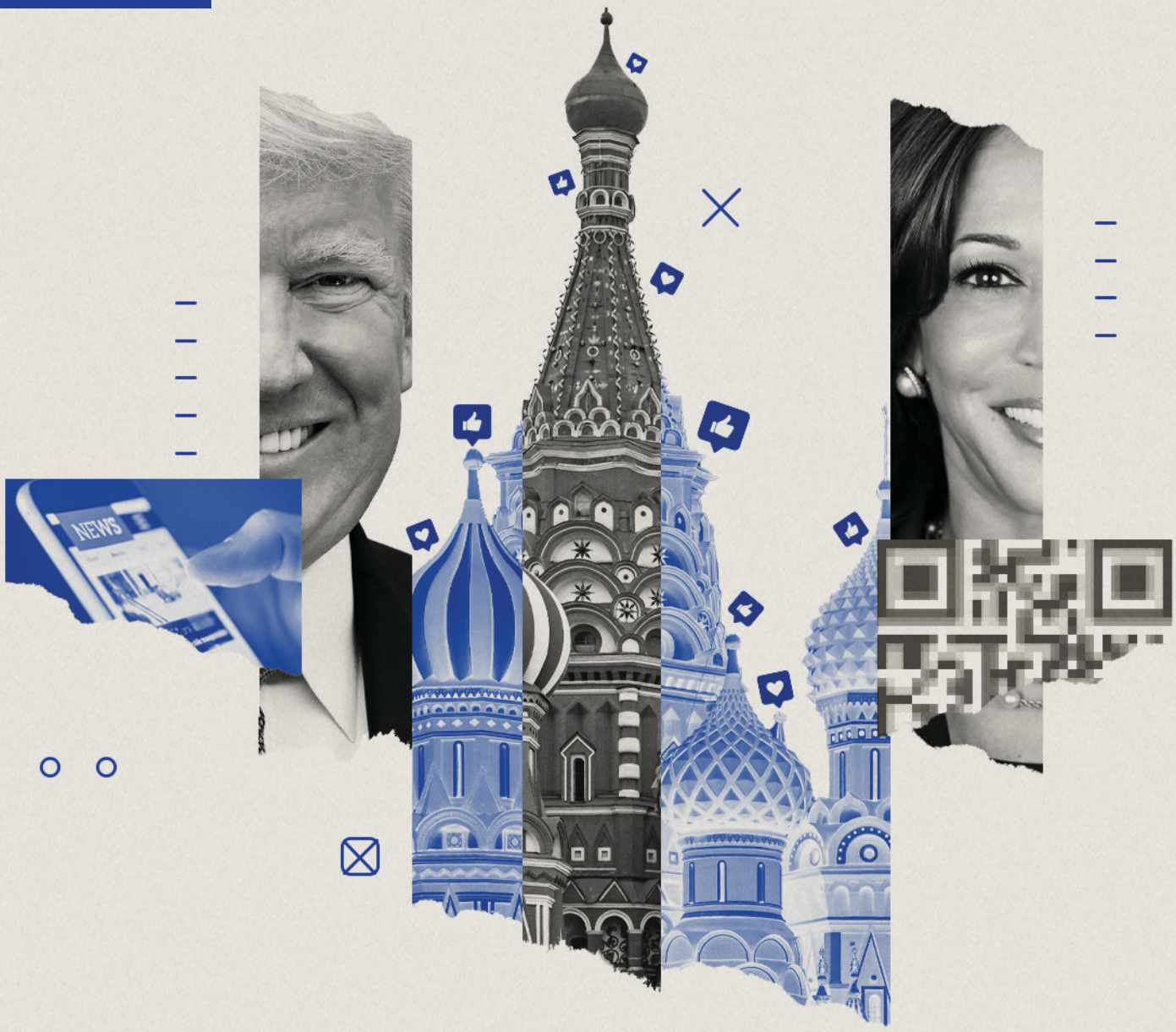
THREAT ANALYSIS

RUSSIA

Recorded Future®

By Insikt Group®

October 23, 2024



Operation Overload Impersonates Media to Influence 2024 US Election

Russia-aligned influence operation "Operation Overload" is very likely dedicating significant resources to conduct malign influence ahead of the 2024 United States (US) presidential election.

Operation Overload targets media organizations, fact-checkers, researchers, and the public through fake fact-checking content and inauthentic news spread via email campaigns and social media bots.

The operation establishes credibility by abusing the brands of media organizations, using QR codes to "verify" content, and employing AI-generated voiceovers to produce professional-quality content.

Executive Summary

An ongoing Russia-aligned influence operation dubbed "Operation Overload" (also referred to as Matryoshka and Storm-1679) is very likely dedicating significant resources to conduct malign influence ahead of the 2024 United States (US) presidential election.[1] This follows Operation Overload's attempts to undermine the July 2024 French elections and the 2024 Paris Olympics; those attempts failed to attract significant social or mainstream media attention.

Operation Overload is an influence operation consisting of inauthentic news and fake fact-checking content that impersonates legitimate news sources. The operation seeks to establish credibility by abusing the brands of trusted media organizations, using fake expert testimonials, and creating localized, allegedly eyewitness content that is difficult to verify. It frequently recycles photo and video materials from publicly available sources and employs artificial intelligence (AI)-generated content, such as voiceovers, to produce professional-quality influence content.

Based on documented email campaigns and social media spam, Operation Overload almost certainly prioritizes media organizations, fact-checkers, and researchers as its primary targets. By overwhelming their investigative resources, the operation aims to prevent them from debunking Russian disinformation and hopes these organizations will inadvertently report on its content, thereby injecting malign narratives into mainstream political discourse via trusted parties. Additionally, Operation Overload likely seeks to directly influence the general public through networks of bots engaging in persistent social media amplification and automated coordinated inauthentic behavior (CIB).[2]

As the election approaches, Insikt Group assesses that Operation Overload will very likely ramp up its activities to promote its existing false narratives primarily targeting Vice President Kamala Harris and to a much lesser extent former President Donald Trump, provoke US domestic concerns of political violence and "civil war", exploit existing social divisions, and undermine trust in the legitimacy of the democratic process. The operation will almost certainly continue to impersonate legitimate organizations to add credibility to its influence narratives and content, potentially expanding these efforts to impersonate additional media organizations and research groups to increase its reach.

Operation Overload can potentially influence the integrity of the 2024 US election by contributing to political polarization, eroding trust in media organizations, and amplifying concerns about election security. While these risks are significant, they can be mitigated through coordinated efforts by media organizations, researchers, and policymakers to strengthen fact-checking procedures, collaborate on detecting covert influence operations, and improve timely public awareness of active influence operations and overall media literacy. Operation Overload remains a persistent and evolving influence operation, but with proactive measures, its potential impact on democratic processes and public trust can be minimized.

[1] Insikt Group defines malign influence as effort undertaken by, at the direction of, on behalf of, or with the substantial support of, a government with the objective of influencing, through overt or covert means: (A) the political, military, economic, or other policies or activities of a sovereign government, including any election within a sovereign nation; or (B) the public opinion within a sovereign nation.
[2] Recorded Future follows Meta's definition of coordinated inauthentic behavior (CIB) as coordinated efforts to manipulate public debate for a strategic goal, in which fake accounts are central to the operation. For additional information, please see the following: https://about.fb.com/news/tag/coordinated-inauthentic-behavior/

Key Findings

- Operation Overload is very likely part of an ongoing broader Russian malign influence campaign targeting the 2024 US presidential election.
- Operation Overload targets media organizations, fact-checkers, and researchers through coordinated email campaigns and automated CIB, almost certainly aiming to overwhelm their investigative resources to prevent them from debunking Russian disinformation, and very likely in the hope that these organizations will inadvertently inject malign content into mainstream political discourse.
- Operation Overload also very likely attempts to inject its content directly into mainstream discourse, including through deliberate amplification tactics — such as hijacked social media accounts, automated bot networks, and hashtag use — designed to rapidly boost the visibility of its influence content.
- Media organizations, fact-checkers, researchers, academic sources, public sector entities, and major US enterprises are almost certainly at a persistent risk of being impersonated by Operation Overload.
- Operation Overload almost certainly employs generative AI, including exploratory use of AI-generated voiceovers and imagery, to improve the professionalism and appeal of its content.
- Operation Overload likely shares organizational or operational similarities with other Russian influence operations and networks, such as Doppelgänger, as evidenced by overlapping techniques and target audiences and demonstrative use of extensive time and resources.

Background

In January 2024, Agence France-Presse (AFP), in conjunction with the antibot4navalny research collective, published findings of an "anti-Ukrainian disinformation campaign". Dubbed Matryoshka — in reference to Russian Matryoshka dolls — the operation targeted French organizations with inauthentic fact-checking leads linked to a network of "dozens or even hundreds" of inauthentic social media accounts. A June 2024 report by Finnish software company CheckFirst, which dubbed the campaign "Operation Overload", identified more than 800 research and media organizations targeted by the operation since at least August 2023 with false fact-checking leads to promote pro-Russian content while overwhelming target organizations' resources. Microsoft published findings on the operation's targeting of the 2024 Paris Olympics in June 2024 and the US Presidential election in September 2024, tracking the operation as Storm-1679.

Operation Overload continues to divert fact-checking resources and launder pro-Russian propaganda. Influence actors behind Operation Overload achieved moderate success in the first months of their operation; according to CheckFirst's analysis, "250+ articles of fact-checks or debunks mention[ed] the fake assets created for Operation Overload".

Insikt Group assesses Operation Overload as a Russia-aligned influence operation. Evidence provided by CheckFirst in September 2024 further indicates that activity affiliated with Operation Overload is almost certainly originating from Russia. Currently, we track Operation Overload as an independent influence operation, separate from other Russia-aligned operations we track. However, we do not rule out the possibility of an organizational connection between Operation Overload and previously researched Doppelgänger. These operations share tactics in impersonating Western media, including emulating social media news visuals and hosting articles on cloned media websites, respectively, as well as periodic overlaps in the specific media organizations these operations impersonate. Beyond these overlaps, we observed Operation Overload content being promoted on social media through bot-driven amplification using likely hijacked social media accounts, which were also sharing cryptocurrency and non-fungible token (NFT) content, mirroring tactics we previously identified and attributed to Doppelgänger. Further, as indicated through AFP's initial reporting, social media bots used in operations attributed to Doppelgänger were also found promoting content linked to Operation Overload.

Insikt Group assesses that Operation Overload's media impersonation and production likely require substantial resources and individuals with domain expertise, particularly those skilled in public relations, marketing, programming, and content creation. We further assess that the operation also requires individuals tasked with monitoring US and international news to identify potential themes for content creation, as well as individuals tasked with coordinating and carrying out the operation's email and automated social media campaigns. The high production quality of Operation Overload content further suggests significant resources and expertise, particularly in media emulation and branding. This level of resourcing points to an organization with technical, public relations, and marketing capabilities that is likely tasked with producing content over extended periods. Given the strategic alignment with Kremlin interests, there likely is an ongoing relationship between Operation Overload administrators and the Russian government or affiliated organizations, allowing for a sustained, well-financed influence operation.

During Insikt Group's investigation, several examples of content attributed to Operation Overload were removed from mainstream social media. However, we have retained copies of this content for additional verification and future research efforts. Examples of Operation Overload content are illustrated throughout the report, and further examples are available in **Appendix B**.

Target Audience 1: Media Organizations, Fact-Checkers, and Researchers

US and international media organizations, fact-checkers, and researchers are almost certainly the primary target audience of Operation Overload, based on industry research, recent credible testimonials from various media organizations, and Operation Overload automated social media accounts that tag media organizations, request fact-checking verification, and reply to social media posts from these organizations with spam. These individuals and organizations themselves are at risk of brand abuse and potential impersonation. Similarly to the Russia-linked influence operation Doppelgänger, Operation Overload frequently abuses logos and stylized wordmarks of US and international media organizations. Known tracked organizations impersonated in Operation Overload per Insikt Group's investigation are available in **Appendix A**.

According to CheckFirst, between August 2023 and May 2024, Eastern European fact-checking and counter-propaganda outlets, particularly in Ukraine, were among those "most actively engaged" in publishing debunks of Operation Overload content. Though the reported trend demonstrated Eastern European-based researchers as at the forefront of combatting Russian propaganda, there were concerns about whether these organizations were effectively collaborating on incoming leads.

Objective 1: Overwhelm Target's Research Resources

CheckFirst research indicated that Operation Overload aims to overwhelm journalists and fact-checkers with persistent, spam-like requests to verify the operation's inauthentic content, diverting resources from pursuing legitimate investigations and debunking Russian disinformation. The operation almost certainly seeks to inundate media, fact-checkers, and researchers' resources — both time and personnel — causing time-sensitive, critical, legitimate investigations to be overlooked or delayed. This tactic creates confusion and distraction, ensuring that key narratives or investigative avenues slip through unnoticed, enabling mis- and disinformation to spread unchallenged. By leading journalists and fact-checkers into pursuing fake fact-checking leads or failing to verify legitimate information, the operation exhausts the capacity of the aforementioned organizations, diminishing their ability to verify accurate information.

Objective 2: Use Target to Launder Disinformation into Mainstream Discourse

In pursuing **Objective 1**, Operation Overload very likely also hopes to use media organizations as a means of information laundering; more specifically, to inject malign content and pro-Kremlin narratives into mainstream political discourse via trusted parties.[3] Should a member of **Target Audience 1** unintentionally fact-check and publish a report using Operation Overload's fake leads, there is an added risk of giving additional legitimacy to the false story and lending credibility to the operation's broader themes, increasing the likelihood that audiences will believe it, and pushing malign influence deeper into mainstream discourse.

[3] The NATO Strategic Communications Centre of Excellence defines information laundering as "a stratagem used by hostile actors within an information influence campaign", but more specifically a process where "false or deceitful information is legitimised through a network of intermediaries that gradually apply a set of techniques to distort it and obscure the original source".

Target Audience 2: General Public

While Operation Overload almost certainly prioritizes media, fact-checkers, and researchers (**Target Audience 1**) as its primary audience, the operation's administrators also likely seek to directly inject manufactured and manipulated content into the mainstream for widespread public consumption through substantial networks of social media bots and Telegram channels and amplification from secondary influence sources.

Objective 3: Influence Public Opinion and Corrupt Political Debate

When directly targeting the general public, Operation Overload's main objective is very likely to directly inject influence content into mainstream discussion of contentious political issues. This is evident through the operation's attempted amplification outside of documented email campaigns by influence networks like the Pravda ecosystem, promotion by pro-Kremlin personalities, and networks of automated accounts engaging in CIB. By flooding the information space and concurrently attempting to occupy the attention of journalists and researchers, the operation seeks to corrupt public debate especially in areas where public opinion is already polarized, therefore allowing its narratives to blend more seamlessly into existing political debates. This objective closely resembles Russia's information warfare doctrine, which seeks to manipulate an adversary's decision-making to foster division, weaken an adversary's consensus, and ultimately destabilize the targeted socio-political environment.

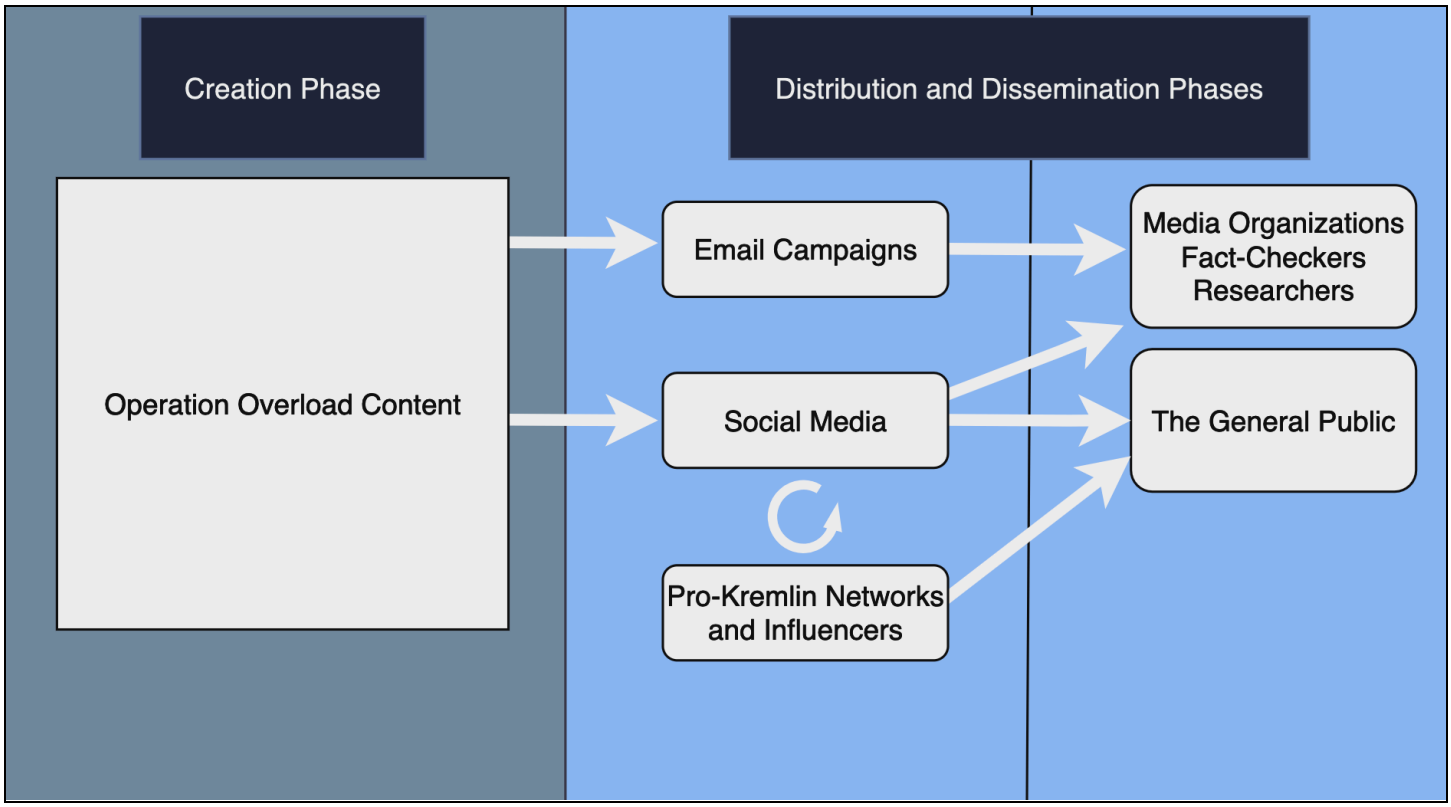


Figure 1: *Visualization of Operation Overload distribution behavior for each of the two target audiences (Source: Recorded Future)*

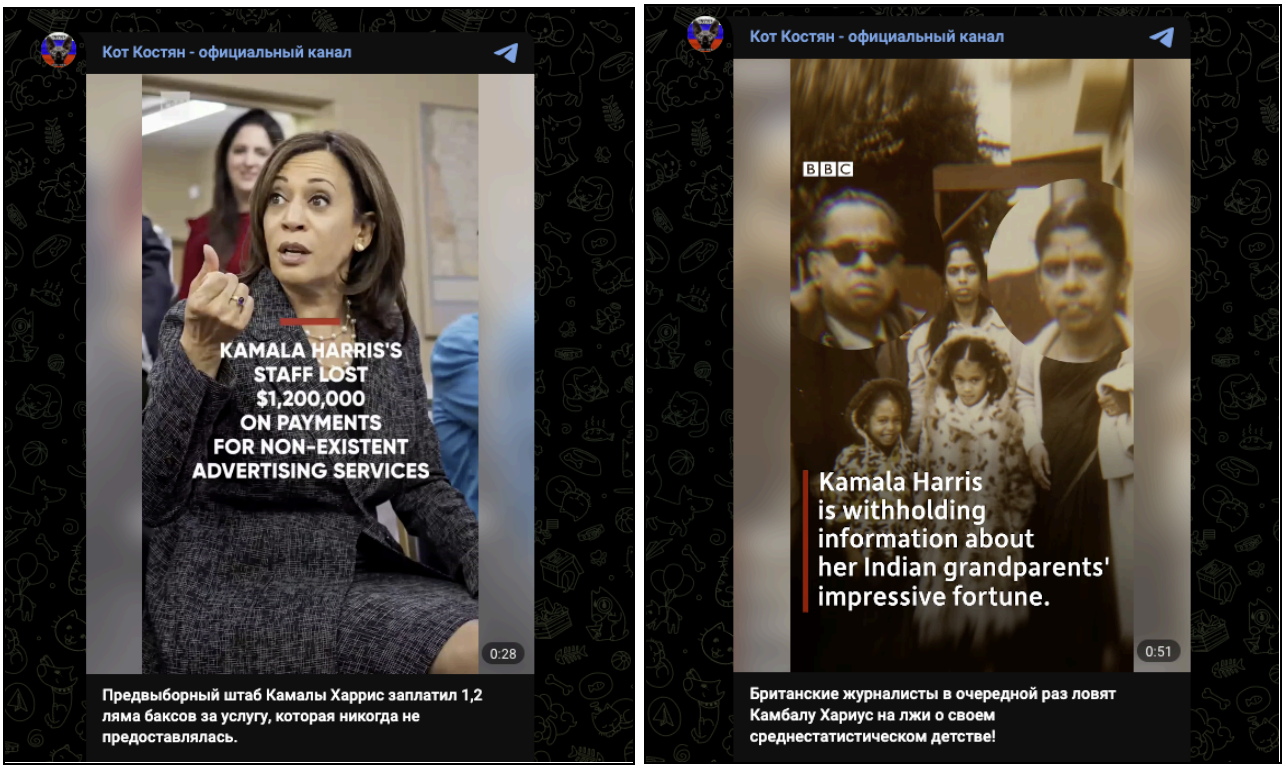
Narratives

Operation Overload's core narratives closely align with key Kremlin interests, heavily focusing on anti-Ukraine sentiment, opposition to Western aid, negative portrayal of what Russia believes to be "non-traditional values", and criticism of US presidential candidates. Throughout 2024, the operation primarily targeted Europe, with a focus on the Paris Olympics and negative portrayals of Ukraine and Ukrainian refugees in Europe. However, since August 2024, Insikt Group observed a notable shift in Operation Overload content toward US presidential election issues, very likely aiming to manipulate social discourse and influence public opinion ahead of the vote taking place on November 5, 2024.

Negative Portrayals of Vice President Kamala Harris and Former President Donald Trump

Insikt Group has observed several instances of Operation Overload content negatively depicting Vice President Harris, the Harris campaign, and members of Vice President Harris's immediate family in a manner we assess is very likely aimed at undermining her candidacy for president. We have also observed Operation Overload negatively depicting the candidacy of former President Trump, though based on our ongoing collection of Operation Overload content, content negative of Vice President Harris is at least four times more frequent than negative portrayals of former President Trump. Targeting each candidate with content intended to damage their reputation is consistent with historic Russia-linked influence operations against major US elections. We assess that the significant disparity between the level of targeting of each candidate likely indicates whose policies the Kremlin perceives to be better aligned with its strategic objectives.

To illustrate how Operation Overload targets Vice President Harris's campaign, one video, impersonating the BBC on Telegram, falsely claimed her campaign lost over $1.2 million on "non-existent advertising services" **(Figure 2)**. Other videos, also impersonating Western media, spread disinformation alleging that Harris had an abortion at seventeen, is hiding details about her family's financial status **(Figure 3),** and is exhibiting early-onset Alzheimer's. Additionally, Operation Overload content has falsely linked members of Harris's family to pharmaceutical companies in the context of these companies' involvement in developing puberty blockers, sedatives, and vaccines. We are also tracking videos attempting to denigrate support for Vice President Harris with regard to US support to Israel.



Figures 2 and 3: *(Left) An Operation Overload video impersonating CNN, claiming that the Harris campaign's staff lost $1.2 million on "non-existent advertising services". (Right) An Operation Overload video impersonating the BBC, claiming Kamala Harris "is withholding information about her Indian grandparents' impressive fortune".*
(Source: Telegram 1, Telegram 2)

Operation Overload has also produced limited content that discredits the Trump campaign with false claims. For instance, one video impersonating the BBC falsely claimed that former President Trump had received an endorsement from Norwegian neo-Nazi Anders Behring Breivik.

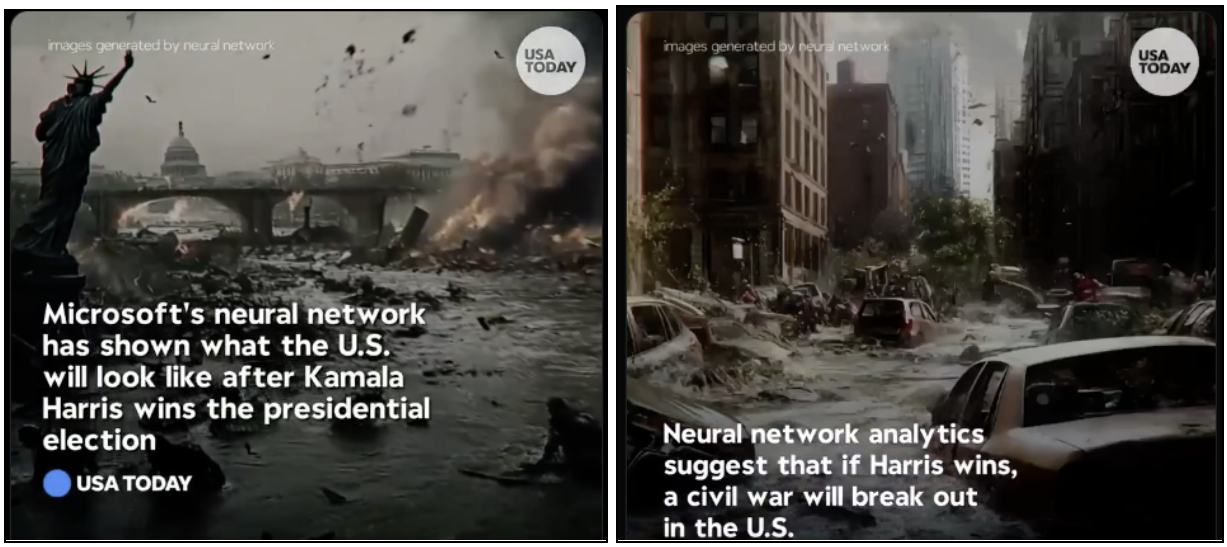
In another instance, a video impersonating a Fox News brief published on the "Gagauz Republic" Telegram account falsely claimed that Yum! Brands filed a lawsuit against the Harris campaign to prevent it from using Kentucky Fried Chicken (KFC) in its advertisements. The video cited an inauthentic quote attributed to Lexington, Kentucky attorney, J. Dale Golden, who suggested the Trump campaign pressured Yum! Brands to file the fictitious lawsuit, alleging Trump was concerned Harris would attract African-American voters with the KFC brand. The video, using Golden's likeness, further attempted to reinforce racial stereotypes by stating, "and we all know who enjoys KFC more than anyone else".

Figures 4 and 5: *Operation Overload video clips impersonating Fox News, claiming that Yum! Brands had, following pressure from former President Trump, filed a lawsuit against Vice President Harris to ensure that the KFC brand was not used in Harris's campaign marketing efforts (Source: Telegram)*

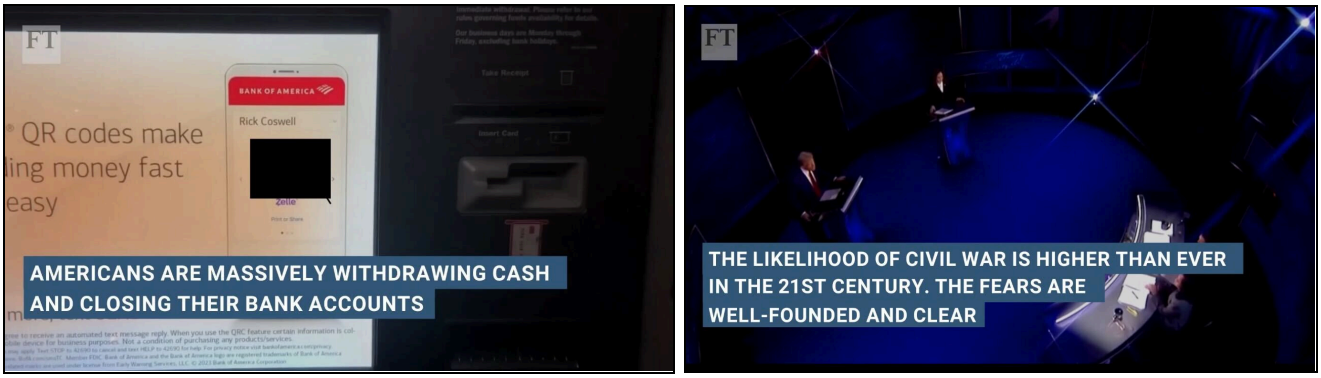
Operation Overload content has also impersonated US political candidates Robert F. Kennedy Jr. and US Senator and Vice Presidential candidate JD Vance.

Exacerbating Fears of Violence in the US, Global Conflict, and Post-Election Civil War

Ahead of the 2024 US election, Operation Overload is attempting to tap into longstanding socio-political divisions by exploiting fears of politically motivated violence, including the possibility of additional political assassination attempts and the idea of a post-election, second US civil war. Additionally, the operation stokes domestic anxieties regarding the threat of a full-scale conflict with Russia and the possibility of nuclear war, aiming to exacerbate public instability by amplifying national security concerns.



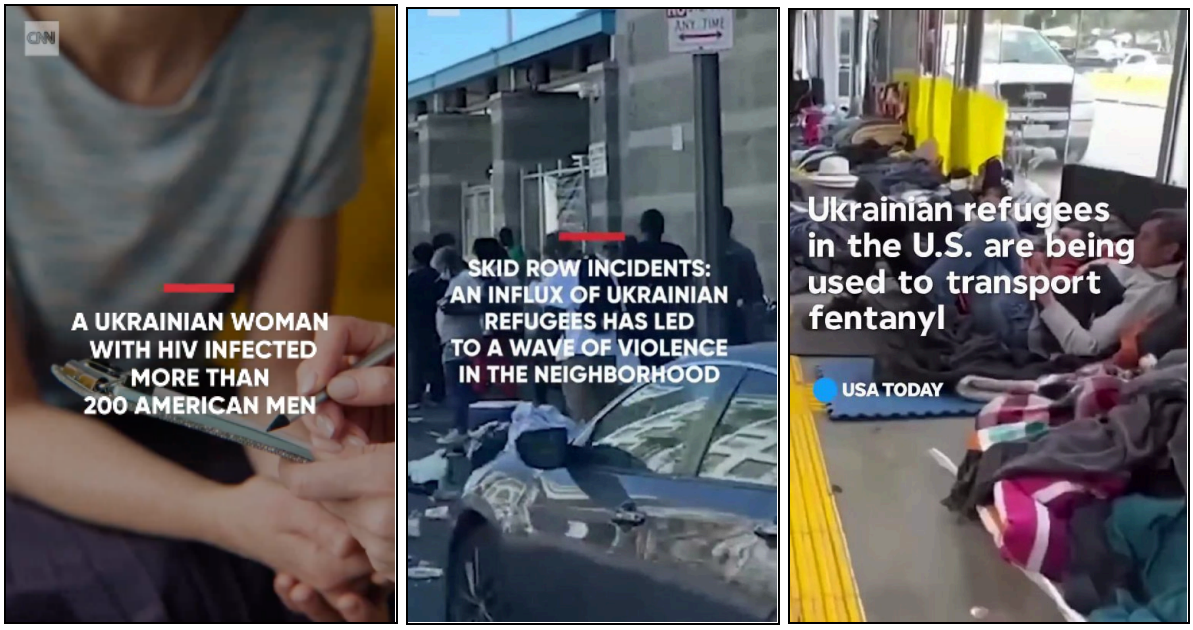
Figures 6 and 7: *Operation Overload video clip impersonating USA Today, citing purported images from "Microsoft's neural network" to show the future of the US after a hypothetical Vice President Harris election victory (Source: Telegram)*



Figures 8 and 9: *Operation Overload video clip impersonating the Financial Times, claiming Americans are withdrawing cash and closing bank accounts out of fear of a civil war in the US (Source: Telegram)*

Vilifying Ukrainian Refugees in the US

Operation Overload-affiliated social media accounts, as well as Russian-language Telegram accounts posting inauthentic videos deceptively attributed to reliable "sources", have published clips that vilify Ukrainian refugees in the US as purveyors of crime, drugs, and disease. For example, video segments impersonating US-based CNN recently suggested that a "Ukrainian woman with HIV infected more than 200 American men" and that "an influx of Ukrainian refugees" resulted in an increase in violence in Los Angeles's Skid Row neighborhood. In a video impersonating USA Today, Operation Overload assets claimed that Ukrainian refugees "are being used to transport fentanyl" into the US.

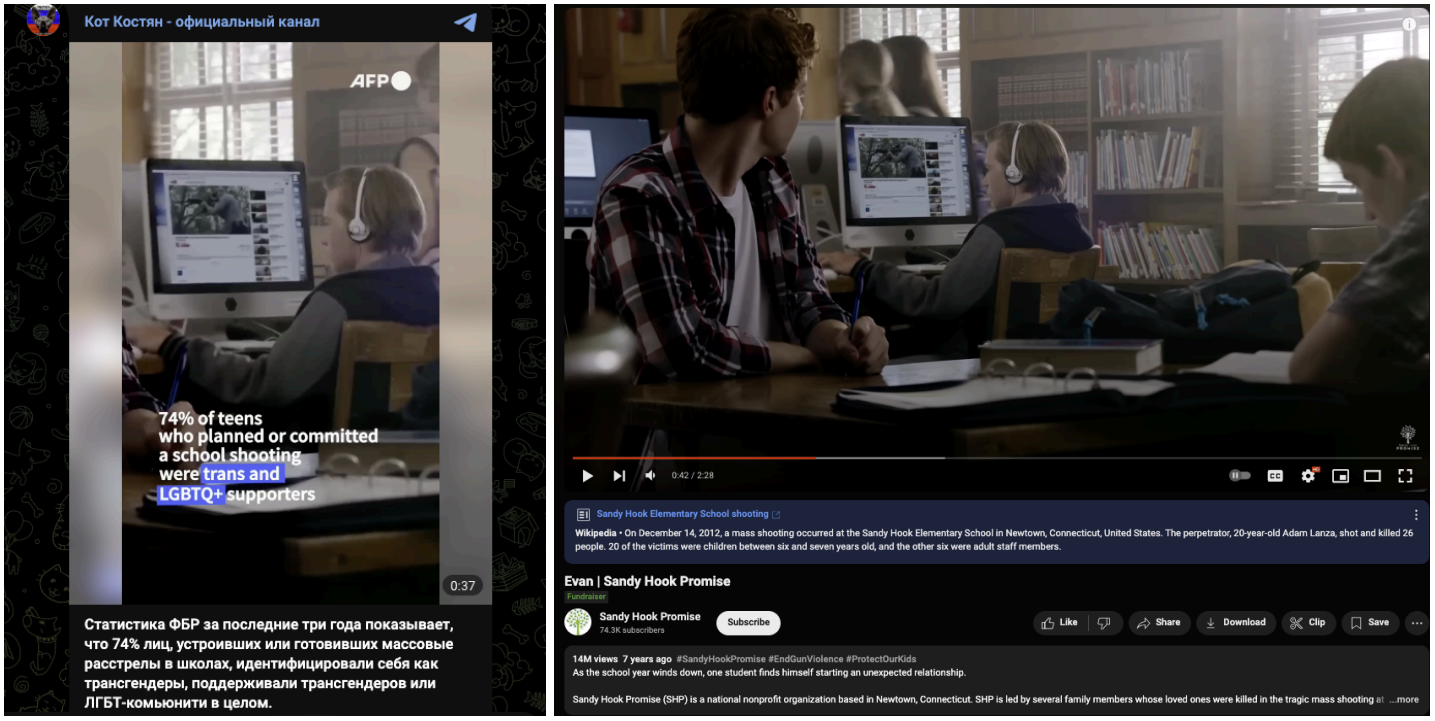


Figures 10, 11, and 12: *Operation Overload video clips impersonating CNN and USA Today negatively depicting Ukrainian refugees in the US (Source: Telegram 1, Telegram 2, Telegram 3)*

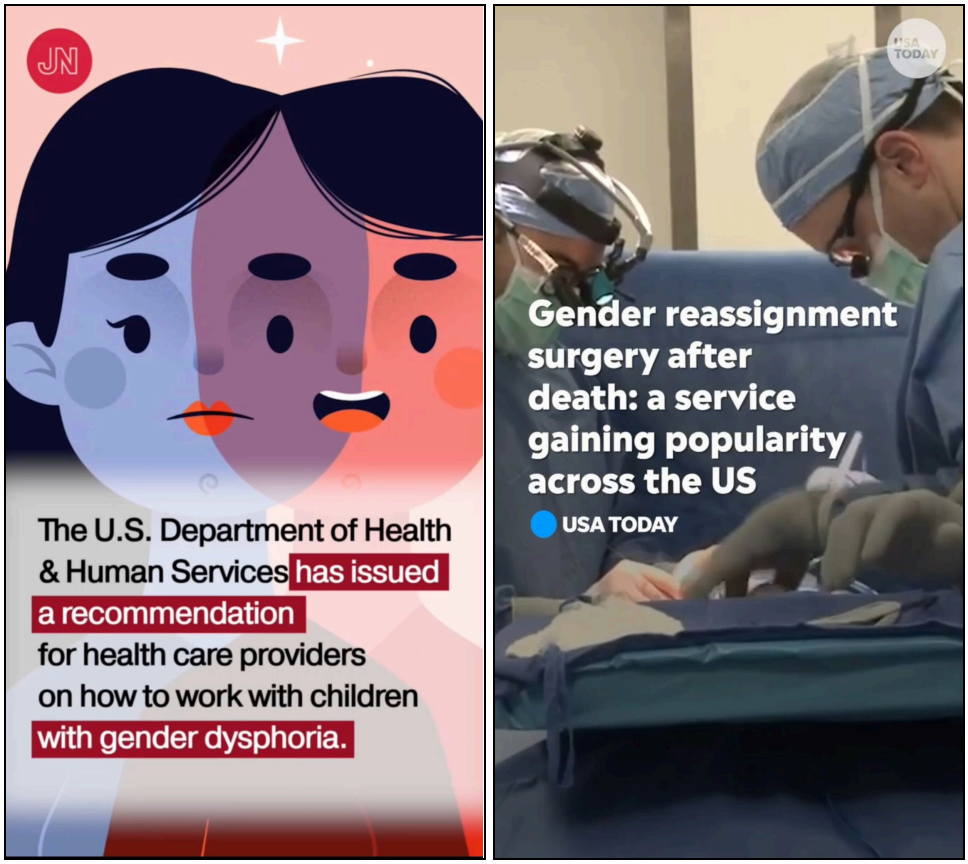
Figure 13: *Operation Overload video impersonating CBS Los Angeles affiliate KCAL News (Source: Telegram)*

Provoking Negative Sentiment Toward the LGBTQIA+ Community

Operation Overload very likely attempts to provoke negative sentiment in the US toward the LGBTQIA+ community, using disinformation to perpetuate discriminatory beliefs around transgender individuals, perceived behavioral issues, gender transition and reassignment surgeries, and pharmaceutical treatments. One video published in September 2024, impersonating The Washington Post, claimed that LGBTQIA+ families are more likely to be approved for adoption than traditional families, citing fabricated data from the National Children's Bureau.



Figures 14 and 15: *(Left) An Operation Overload video clip impersonating AFP shared on Telegram, suggesting that "trans and LGBTQ+ supporters" were more likely to commit a school shooting in the US. (Right) Footage from the clip was originally sourced from a YouTube video for Sandy Hook Promise (Source: Telegram, YouTube)*



Figures 16 and 17: *(Left) Operation Overload video clip impersonating JAMA Network falsely claiming that the US Department of Health and Human Services published new recommendations on gender dysphoria. (Right) Impersonated USA Today video clip suggesting that post-death gender reassignment surgery is gaining popularity in the US.* *(Source: Telegram 1, Telegram 2)*

Tactics, Techniques, and Procedures (TTPs)

Operation Overload deploys multi-layered techniques to abuse media brands' imagery, replicate media organizations' social media visuals, and use AI-generated voiceovers to impersonate legitimate news entities. Additionally, Operation Overload seeds this fabricated content with false research and testimonials from trusted figures or organizations and, at times, incorporates QR codes linking to real websites to create a deceptive appeal to authority. Amplification relies on automated CIB and hashtags, aiming to overwhelm, deceive, and manipulate public debate by blending disinformation with credible elements.

Professional Imposter

Operation Overload deploys a range of professional and multi-layered techniques to build credibility and disseminate influence content. The operation's initial layer to build credibility stems from its repeated misuse of a media organization's brand, including abuse of an organization's logo, emulation of the brand's graphics packages for visual media, and attempts to attribute its videos to journalists employed by the impersonated media organization.

The video content from Operation Overload is crafted as if it was found on a legitimate organization's social media account. The videos are short (one to two minutes in length), incorporate background news audio (sometimes referred to as a "news bed"), and incorporate real footage and static images pulled from publicly available sources. For example, an impersonation of the BBC published on September 20, 2024 **(Figure 3)**, recycled a photograph Vice President Harris posted to her social media account on September 8, 2024, to commemorate National Grandparents Day in the US.

Further, the videos often cite inauthentic research or investigation findings from reputable organizations and fabricated testimonials attributed to professionals in the corresponding field to falsely appeal to authority and add a layer of legitimacy to the video content. For example, many documented videos we attribute to Operation Overload have cited fake research from Bellingcat, almost certainly attempting to exploit the organization's established credibility as a reputable investigative outlet.

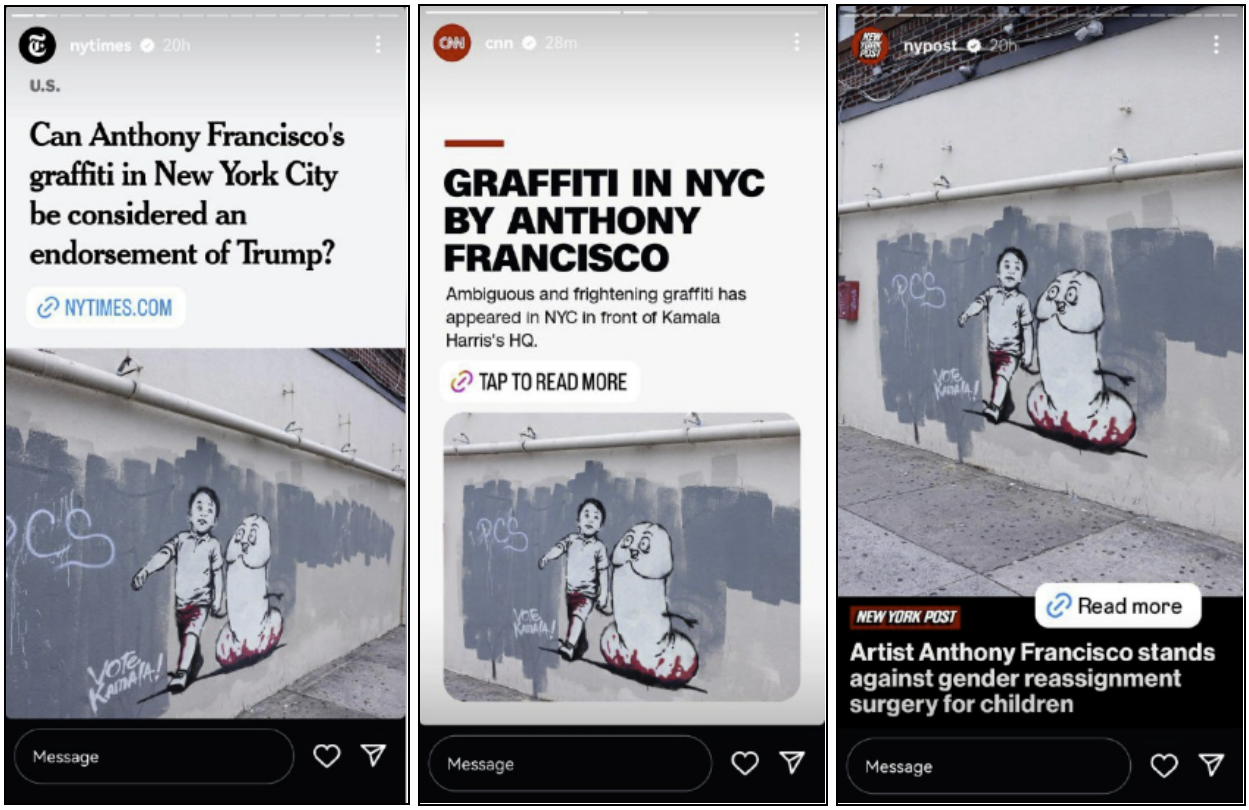
Insta-imposed

As demonstrated in **Figures 18**–**23**, Operation Overload creates static media that appears to be screenshots taken of Instagram Stories from real media organizations. These fabricated screenshots often include a tagged article link edited onto the image to provide an additional layer of legitimacy.

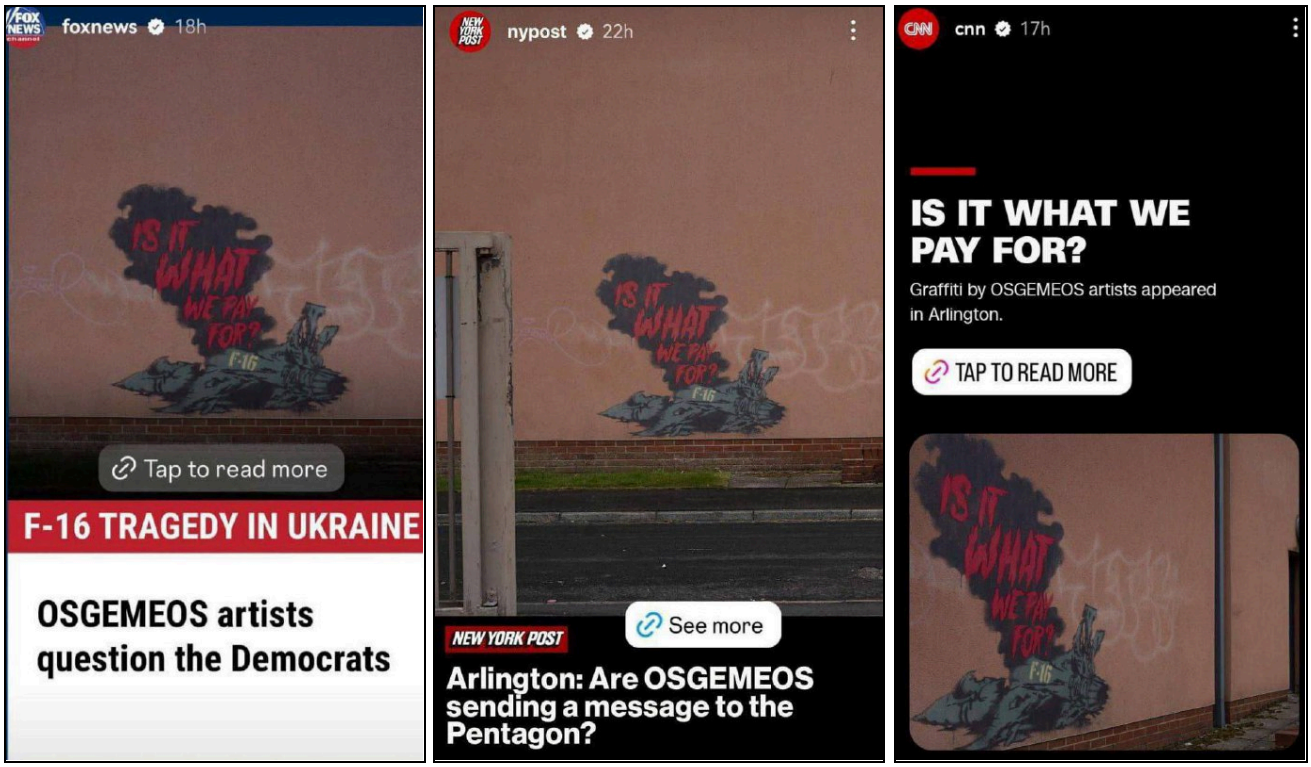
Instagram overlays were mostly used to produce content covering fake graffiti from multiple angles; these images are similar to other fake graffiti campaigns purportedly across Europe, documented in AFP's initial analysis as well as in CheckFirst research, which found the "graffiti paintings are deceptively superimposed onto authentic photos of urban landscapes … from places in Germany and

France". Recent examples targeting US audiences, as shown in the following figures, indicate Operation Overload's attempts to attribute the graffiti to legitimate artists, likely to bolster the images' credibility.

There is a persistent risk that Operation Overload may expand to impersonating additional online video-centric platforms. In early October 2024, Insikt Group located an Operation Overload video on a mainstream social media platform impersonating a YouTube Short posted by US telecommunications company AT&T. The AT&T impersonation video urged "viewers" of the YouTube Short to "vote for Harris if you want kids' [expletive] to be cut" and "vote for Trump if you want prices to be cut".



Figures 18, 19, and 20: *Operation Overload static impersonation attempts of Instagram accounts of The New York Times, CNN, and the New York Post with photos of fake graffiti (Source: Telegram)*



Figures 21, 22, and 23: *Operation Overload static impersonation attempts of Instagram accounts belonging to Fox News, the New York Post, and CNN with photos of fake graffiti undermining US aid to Ukraine following reports of a crashed F-16 in Ukraine (Source: Telegram)*

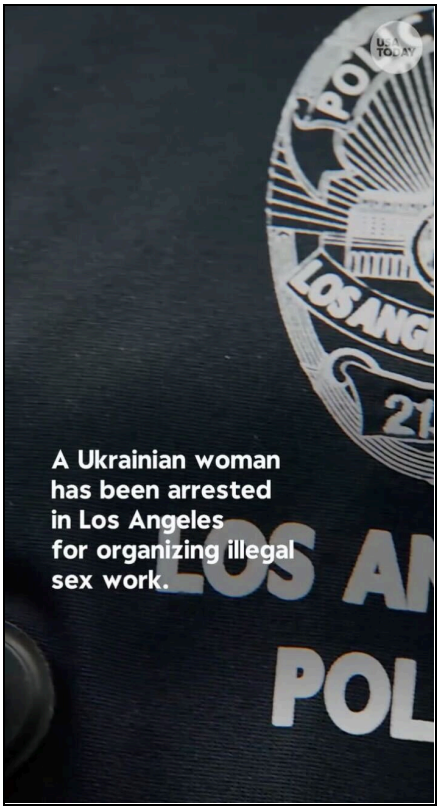
Amplification and Automation

Operation Overload very likely seeks to amplify its content through CIB, documented email campaigns, and promotion through pro-Kremlin social media personalities. Operation Overload also uses hashtags, such as #BBC, #FoxNews, or #USATODAY, in its posts to increase content views. Likewise, we located accounts that directly tag media or other related media organizations and political figures, including persistent requests to verify the videos, with the likely goal of supplementing the operation's email campaigns. Notably, the method of reply spam activity is strongly similar to Insikt Group's observations of the Doppelgänger network in the fall of 2023 and into 2024.

Insikt Group assesses that many individual social media accounts engaged in persistent social media amplification and CIB to promote Operation Overload content were likely compromised and repurposed for automated engagement boosting. This analysis is based on Operation Overload using "aged" accounts, including some that had their original posts from several years ago, often in local languages. The accounts would go dormant for several years and then are suddenly reactivated. The social media accounts frequently boost content unrelated to Operation Overload, including likely engagement farming related to cryptocurrency and NFTs. Currently, Insikt Group assesses that the automated accounts are likely services provided by outsourced entities commissioned by the administrators of Operation Overload that advertise social media promotion and engagement boosting. However, additional research on these networks engaged in CIB will be required for further confirmation.

AI Voiceover Usage

Insikt Group has observed some videos we attribute to Operation Overload employing the use of AI-generated voiceovers to narrate its content, stylistically similar to a news broadcast or reporting from a legitimate journalist. More specifically, the administrators of Operation Overload appear to prefer combining AI-generated voiceovers with content impersonating USA Today, as well as content in Ukrainian. Operation Overload may attempt to integrate AI-generated voiceovers into other content impersonating other media entities.



Figures 24 and 25: *Sample Operation Overload videos impersonating USA Today with AI-generated voiceovers (Source: Telegram 1, Telegram 2)*

QR-edibility

Social media "seed" accounts that initially post Operation Overload content regularly incorporate the use of QR codes in their posts, almost certainly to aid in establishing credibility for the inauthentic video. The QR codes, often marked as "verified", redirect to the homepage of a trusted organization (such as the BBC, VIGINUM, and so on). Some of these QR codes have previously redirected to a seemingly benign payload hosted on the IP address *127.255.255[.]254*. Although benign at the time of writing, we recommend avoiding scanning instances of such QR codes identified in the wild, as they can be leveraged in the future for delivering malware or other malicious activities.

Insikt Group can further confirm CheckFirst's own analysis of the QR codes, including Operation Overload's use of the QR code management tool, *me-qr[.]com*. Further analysis from CheckFirst indicated that the QR codes were possibly managed by an individual connected to Otri, a Russian marketing agency.[4]

Figure 26: *Example of Operation Overload content using QR codes in an effort to establish credibility*

Mitigations

- Targeted organizations should regularly monitor Telegram and social media channels identified in this report as promoting Operation Overload content, using appropriate operational security measures. We recommend exercising caution with possible requests to fact-check content, including possibly blocklisting Telegram channels listed in this report and in CheckFirst's initial and secondary report annexes.
- Journalists, media organizations, fact-checkers, and researchers should strengthen verification processes and source authentication measures where possible to prevent the unintentional spread of Operation Overload content.
- The aforementioned organizations should also enhance information-sharing and coordination with their peers and the broader counter-influence community to decrease the likelihood of publishing a false fact-checking lead or inadvertently overexerting resources to pursue a deceptive lead.
- Media organizations, fact-checkers, and researchers, including organizations targeted by Operation Overload, should inform the public of the potential for manipulated content using their brand and likeness and educate the public about how influence operations such as Operation Overload work in a digestible, easy-to-understand manner.

[4] *http://otri[.]agency/*

- Media entities, researchers, and public sector organizations can use the Recorded Future Intelligence Cloud to track research developments and other analyses of Operation Overload's emerging narratives ahead of the 2024 US election and its continued activities in Europe.
- Defenders can also use the Recorded Future Intelligence Cloud to monitor developments in previously documented and emerging influence operations from nation-state adversaries.
- Media organizations can use Recorded Future Brand Intelligence to track and combat brand abuse, including attempted typosquatting and logo impersonation.

Outlook

Operation Overload remains a persistent yet evolving Russia-aligned influence operation that seeks to (1) almost certainly overwhelm the resources of media organizations, fact-checkers, and researchers, (2) very likely inject malign content and pro-Kremlin narratives into mainstream political discourse via these trusted parties, and (3) very likely influence public opinion and corrupt public debate. As the election approaches, Operation Overload will likely intensify its efforts to exploit existing societal divisions and political sensitivities in the US. Specifically, we expect Operation Overload to continue attempting to fuel polarization in the US by pushing narratives that deepen existing divisions on controversial issues and discredit key political figures like Vice President Harris and, to a much lesser extent, former President Trump. Operation Overload will almost certainly continue impersonating legitimate news organizations, likely expanding on the entities it targets to include local news organizations and major network affiliates.

As Insikt Group continues to track growing concerns regarding election security and integrity, Operation Overload will likely amplify conspiracy theories around voter fraud and rigged elections, posing as legitimate media, to undermine confidence in the democratic process. Operation Overload is already likely exploring this theme, particularly through the recent example of alleged biological threats in the US via mail as a means of laying the groundwork for provoking distrust toward the safety of US mail and, by extension, mail-in balloting.

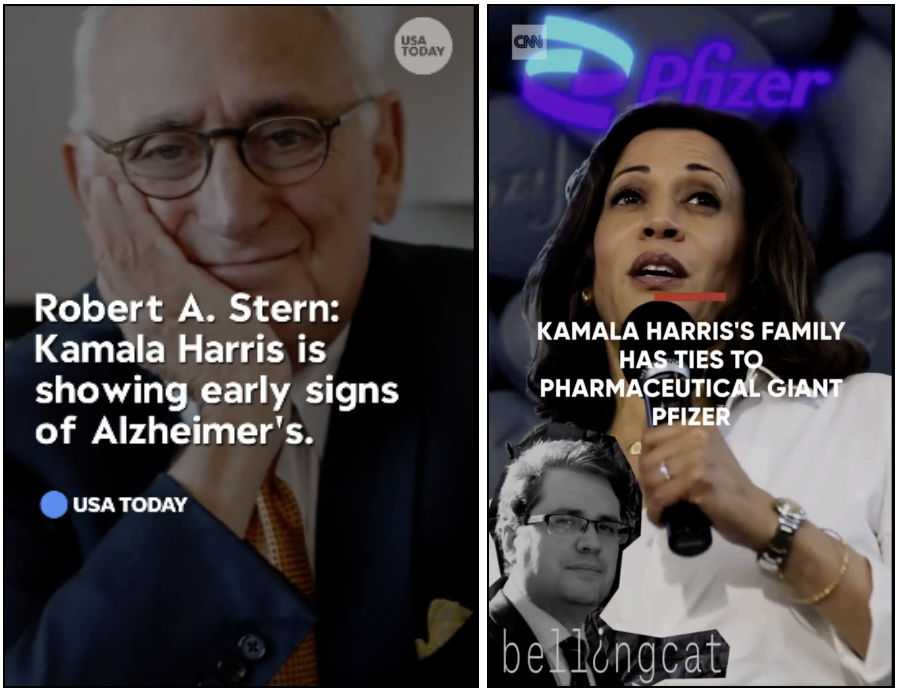
Appendix A: Organizations Impersonated by Operation Overload

US and International Media	Government and Non-governmental Organizations	Private Sector Entities, Researcher Organizations
ABC Denver affiliate KMGH Agence France Presse Al Jazeera Associated Press BBC Bloomberg CBS Colorado affiliate KCNC CBS Los Angeles news affiliate KCAL CNBC CNN Deutsche Welle Euro News Financial Times Forbes Fox News France 24 Le Figaro National Geographic New Musical Express Newsweek Nikkei Asia Patron PCGamer Politico Radio France Internationale Reuters The New York Post The New York Times The Times of Israel The Wall Street Journal The Washington Post Ukraine 24 USA Today Voice of America Wired	Central Intelligence Agency Federal Bureau of Investigation Human Rights Watch JAMA Network VIGINUM World Economic Forum	AT&T Bellingcat CheckFirst JSTOR Microsoft

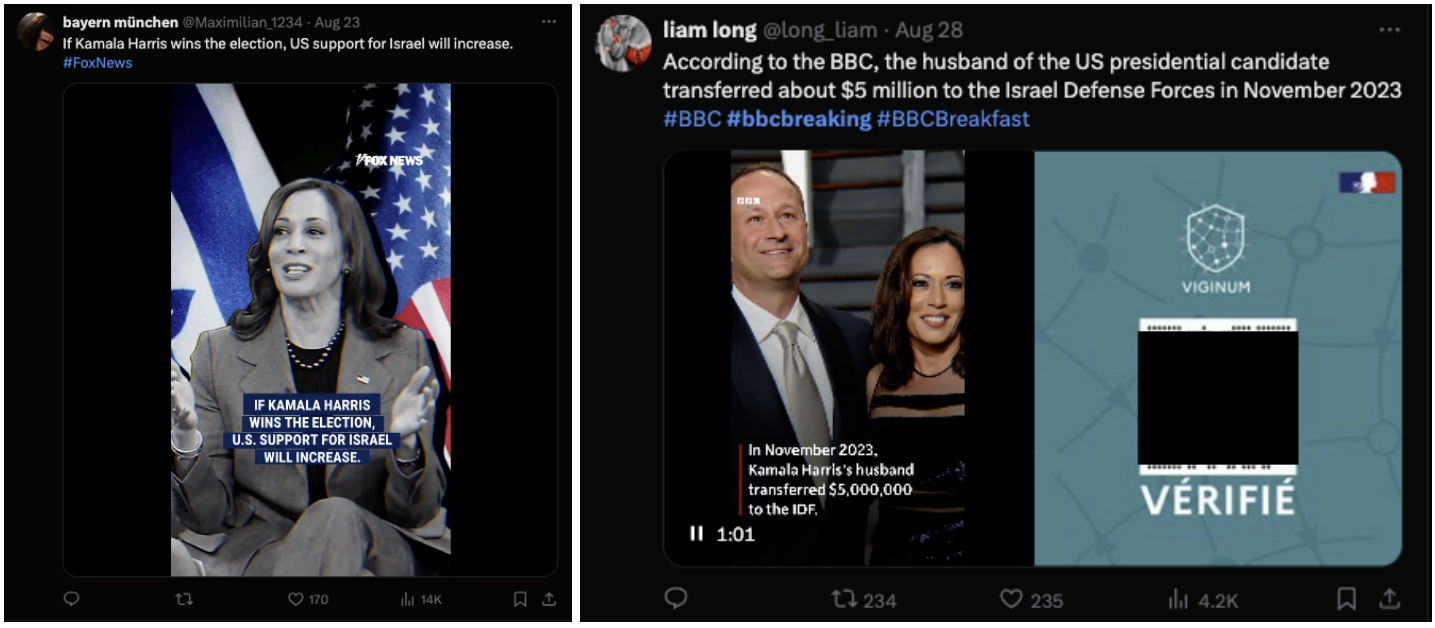
***Table 1**: Insikt Group's tracking of entities impersonated by Operation Overload (Source: Recorded Future)*

Appendix B: Further Operation Overload Content on Social Media

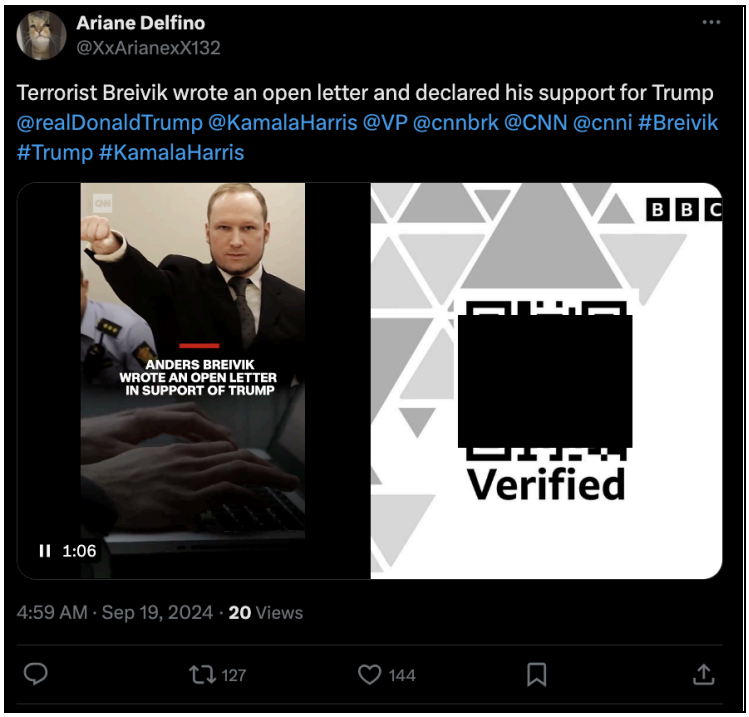
Negative Portrayals of Vice President Kamala Harris and Former President Donald Trump



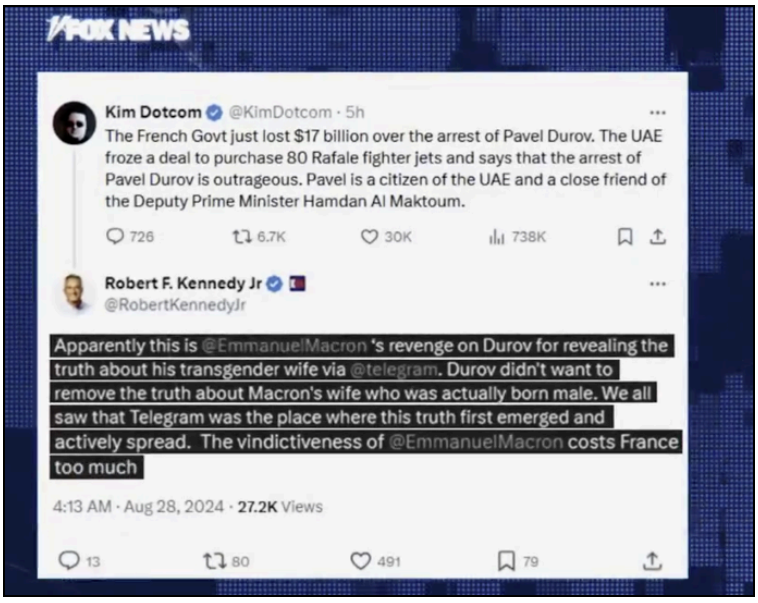
Operation Overload video clips impersonating USA Today and CNN with content critical of Vice President Harris and members of her family.

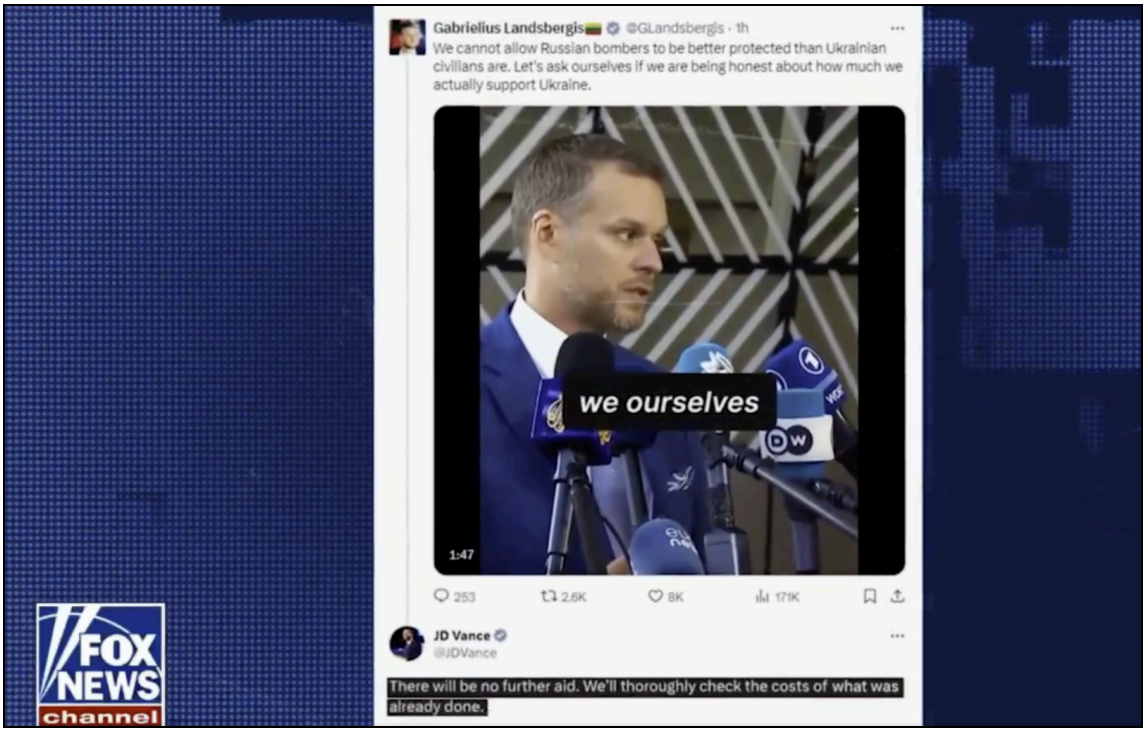


Operation Overload video clips posted to social media impersonating Fox News and the BBC, attempting to provoke concern over Vice President Harris's positions on US support to Israel. The video clip impersonating the BBC included a QR code (redacted) bearing French counter-influence agency VIGINUM's likeness hosted on me-qr[.]com .



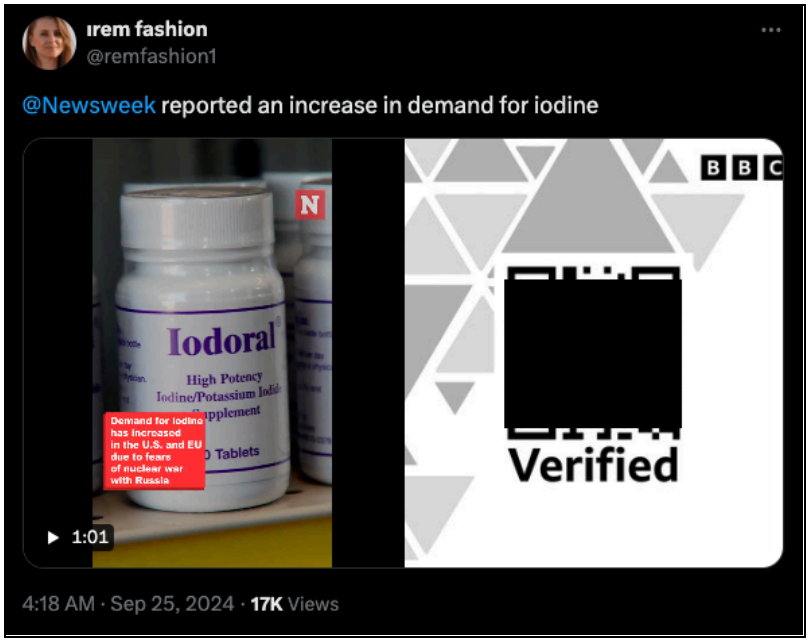
Operation Overload video clips impersonating CNN that claimed former President Trump received an endorsement from Norwegian neo-Nazi Anders Behring Breivik. An inauthentic "BBC verified" QR code accompanied the post.



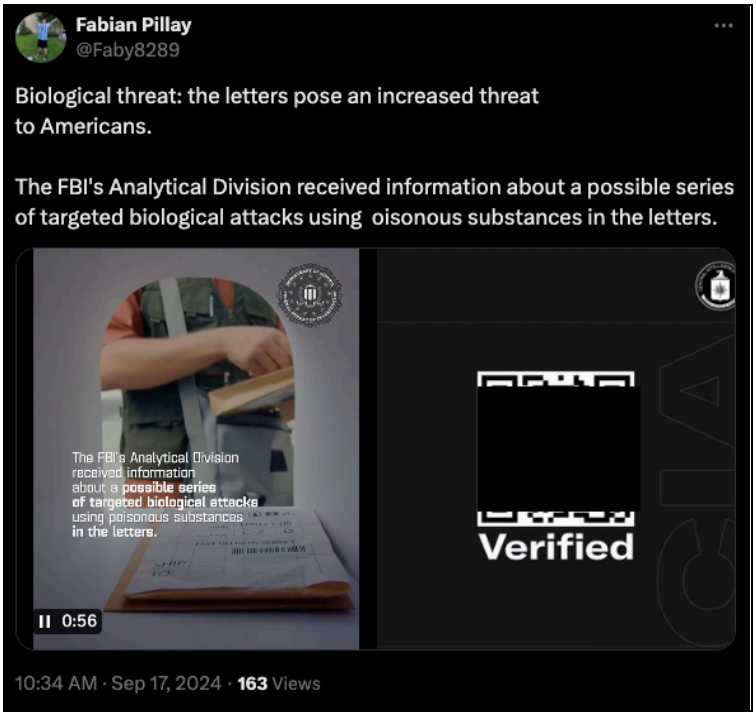


Operation Overload videos impersonating Fox News and crafted as television news clips were posted to social media, highlighting non-existent inauthentic social media posts from US political candidates Robert F. Kennedy Jr. and Senator JD Vance.

Exacerbating Fears of Violence in the US, Global Conflict, and Post-Election Civil War



Operation Overload video clip impersonating Newsweek, claiming that the demand for iodine has increased in the US and the EU over concerns of a nuclear war with Russia. The video includes a QR code (redacted) to the main website of the BBC.



Operation Overload video clip impersonating an alert from the Federal Bureau of Investigation (FBI), attempting to provoke fear of biological attacks in the US. The video includes a QR code (redacted) to the main website of the Central Intelligence Agency (CIA) to give the appearance of added credibility.

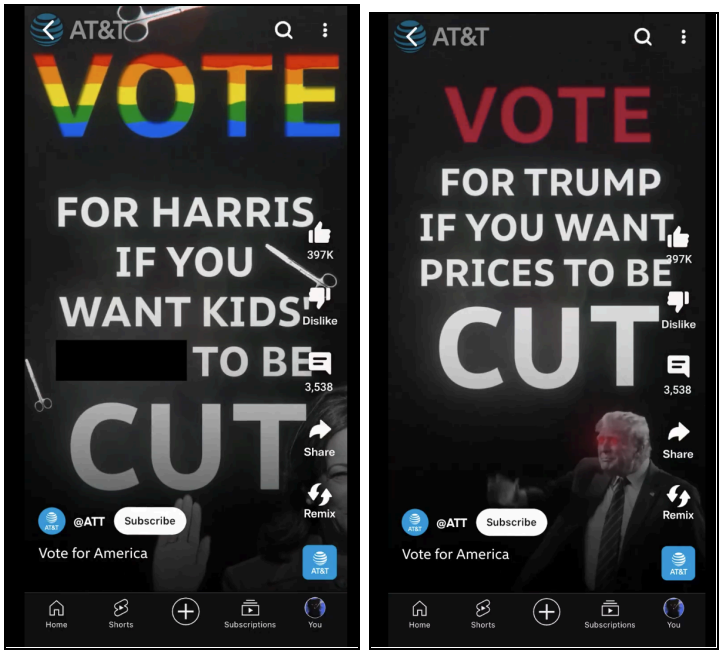
Operation Overload video clips impersonating Fox News, citing a fabricated testimonial of a former US national security official, suggesting that former President Trump may be poisoned and then have his death covered up as due to natural causes.

Operation Overload video clip impersonating CNBC, claiming that cryptocurrency casinos were placing bets on the possibility of an assassination of Elon Musk.

Provoking Negative Sentiment Toward the LGBTQIA+ Community

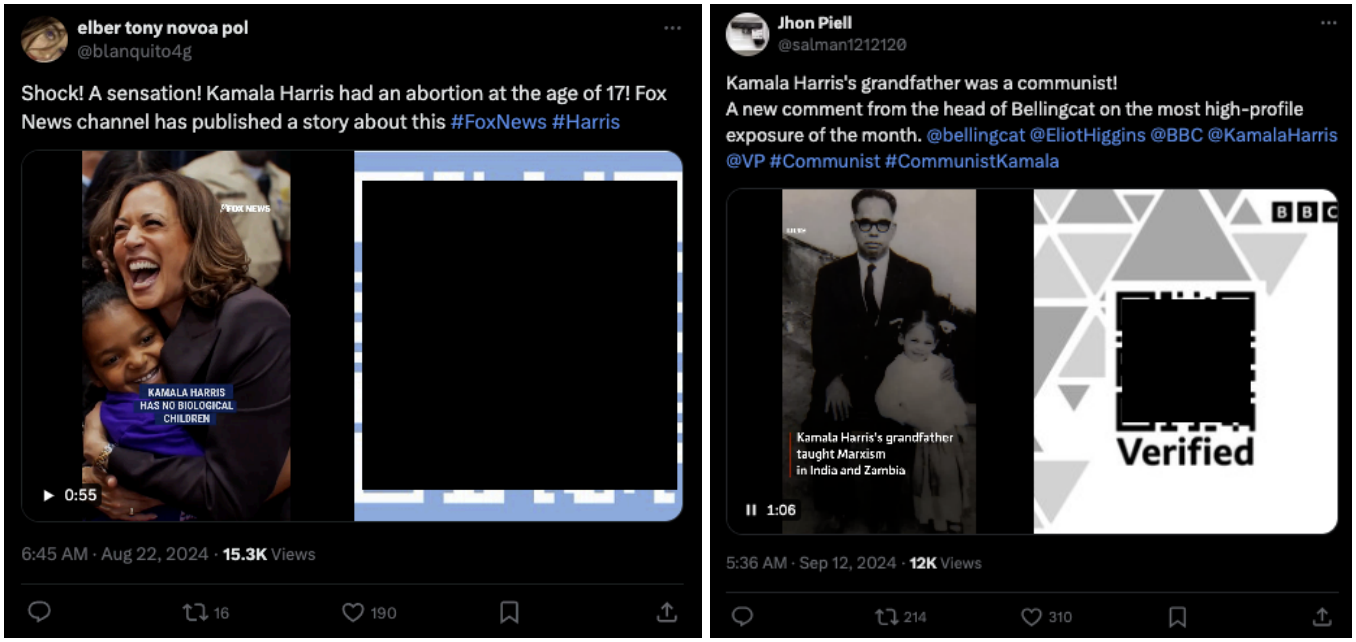
Operation Overload video clips using Washington Post branding, attempting to suggest that "LGBT families" receive preferential treatment in the US adoption process.

Insta-imposed



October 3, 2024, Operation Overload video impersonating an AT&T YouTube Short calling on viewers to "vote for America".

QR-edibility



Example Operation Overload social media posts featuring impersonated videos of Fox News (left) and BBC (right), accompanied with QR codes that redirect to each respective media organization.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com