

“Operation Undercut” Shows Multifaceted Nature of SDA’s Influence Operations

Russia’s Social Design Agency (SDA) is almost certainly conducting an influence operation tracked by Insikt Group as “Operation Undercut” since at least December 2023.

Operation Undercut’s main objective was almost certainly to weaken Western support for Ukraine and exacerbate domestic and international anxieties around the 2024 US elections.

The network uses video content with AI-generated voiceovers and images that reference real articles by Western media outlets, similar to Doppelgänger and Operation Overload.

Executive Summary

Russia's Social Design Agency (SDA) is almost certainly conducting an influence operation tracked by Insikt Group as "Operation Undercut" since at least December 2023, demonstrating SDA's operational capability to conduct multiple influence operations in tandem to support Russia's Presidential Administration's global influence objectives. The SDA is a Moscow-based company accused by the United States (US) government of running Doppelgänger, a [persistent](#), multi-platform influence operation active since 2022. While Insikt Group found significant continuity between Operation Undercut and Doppelgänger — such as narratives, target audiences, and the visual style of certain assets — these networks use separate infrastructure, social media accounts, and delivery mechanisms to reach target audiences.

Based on [leaked SDA documents](#), a US Department of Justice (DOJ) [affidavit](#), and previous [reporting](#) by OpenAI, Operation Undercut is almost certainly an SDA-run influence operation, which likely remains distinct but running in parallel with Doppelgänger. In contrast to Doppelgänger's use of inauthentic websites, Operation Undercut primarily uses artificial intelligence (AI)-enhanced videos and images impersonating major news organizations to amplify its narratives, which it amplifies using trending hashtags in target countries. These tactics are similar to [Operation Overload](#) (also tracked as Matryoshka), another Russian influence operation that shares infrastructure with Doppelgänger.

Operation Undercut has generated very little online engagement and very likely has achieved minimal impact on public opinion. Despite this, like other Russian influence operations, Operation Undercut's main objective is almost certainly to weaken Western support for Ukraine, which it does by attempting to discredit Ukrainian leadership, convince Western audiences of Ukraine's failure to employ Western aid appropriately, and enhance the perception of Russian military operations as being successful. Operation Undercut accounts also developed a narrative that both Ukraine and Israel's futures hinged on the results of the 2024 US elections, in an attempt to exacerbate domestic and international anxieties around those elections. Other narratives include attempts to: exploit existing tensions between the European Union (EU) and its member states, including on the subjects of aid to Ukraine and Russian sanctions; exacerbate tensions over the Israel-Gaza conflict; and criticize the 2024 Paris Olympics.

News and media organizations play a key role in investigating and publicizing influence operations; however, these organizations must also proactively monitor brand impersonations, particularly when they are consistently abused by influence operations like Operation Undercut, Operation Overload, and Doppelgänger to gain credibility. Brand abuse in the context of influence operations can also lead to reputational damages, contribute to the erosion of consumer trust, and deter advertisers, thereby inflicting financial harm on the impersonated organizations.

Influence operators' steady adoption of emerging technologies such as generative AI also means that, while commercial providers have played a key role in investigating covert influence operations abusing their products, including Doppelgänger and Operation Undercut, they must continue to proactively

monitor, block, and deter abuse to prevent adversaries benefiting from these technologies' [scaling and personalizing](#) effects for malicious use.

Key Findings

- Insikt Group identified a network of over 500 social media accounts on multiple platforms operating since at least December 2023, which we track as Operation Undercut. We suspect that the number of accounts in this network is likely much larger, some of which have already been taken down by social media platforms.
- Operation Undercut promoted narratives in continuity with Doppelgänger, including discrediting Ukraine's political and military leadership, attempting to undermine Western military aid to Ukraine, and framing the future of this aid as dependent on the result of the 2024 US elections.
- Operation Undercut also attempted to widen existing socio-political divisions, including in countries like the US, over topics like the Israel-Gaza war and assassination attempts on former President (now President-Elect) Trump.
- The EU and European citizens were recurring targets of Operation Undercut, with content attempting to exacerbate existing tensions between member states and Brussels and discredit EU leaders.
- Operation Undercut's tactics mostly revolve around producing AI-enhanced videos, which are very likely produced using several commercial AI tools, including ElevenLabs, to generate voiceovers.
- Accounts also posted images, including screenshots of articles from major Western news and media outlets, often taking Western leaders' quotes about Ukraine out of context to frame them as anti-Ukrainian narratives.

Table of Contents

Background	4
Attribution	5
Operation Undercut and Doppelgänger: Likely Separate Operations Conducted by SDA	5
Operation Undercut Is Almost Certainly an SDA-Run Operation	7
Identical Visual Content with Leaked SDA Documents	8
Network Coordination	9
Narratives	10
Undermining Western Support to Ukraine and Ukrainian Leadership	11
Exacerbating Tensions over the Israel-Gaza Conflict	12
Escalating Internal EU Tensions	13
Framing Global and Domestic Conflict as Dependent on the 2024 US Elections	15
Criticizing the 2024 Paris Olympics	18
Tactics, Techniques, and Procedures (TTPs)	19
AI-Enhanced Video Content	19
Impersonating and Framing Legitimate Media Content	20
Localized Hashtag Use	21
Alternate Social Media Platforms	22
Amplification of CopyCop Content	23
Mitigations	24
Outlook	24

Background

This report analyzes a Russian influence operation Insikt Group tracks as Operation Undercut, which was partially [documented](#) and attributed to SDA's Doppelgänger operation by OpenAI in May 2024, in addition to previous reporting on aspects of the operation by [Reset Tech](#) and the Institute for Strategic Dialogue. However, our broader scope of investigation leads us to assess that this cluster of activity is likely parallel to but distinct from known Doppelgänger activity, given the divergence in content production, social media accounts, infrastructure, and delivery mechanisms between the two operations.

On May 30, 2024, OpenAI [reported](#) on Doppelgänger's use of ChatGPT via Russian and Czech proxy services to generate content posted on 9gag (a Hong Kong-based social media platform). OpenAI attributed the posts to Doppelgänger by observing accounts using ChatGPT to generate and translate comments posted alongside inauthentic websites previously [attributed](#) to Doppelgänger. However, Insikt Group identified this 9gag content as being part of a broader, multi-platform cluster of influence activity, which we track as Operation Undercut. OpenAI's report also noted that "each cluster displayed different tactics, techniques and procedures (TTPs), consistent with an operation made up of different functional teams", suggesting that SDA's activities are unlikely to be monolithic, and instead reflect distinct operations with different uses for the company's products.

On September 4, 2024, the US DOJ [announced](#) the seizure of 32 Doppelgänger domains and unveiled an affidavit describing the activities of Russian companies SDA, Structura, and ANO Dialog and confirming their involvement in creating and operating Doppelgänger, a persistent influence operation.

On September 16, 2024, journalists from [Vsquare](#), [Delfi Estonia](#), [Radio Svoboda](#), [Süddeutsche Zeitung](#), and [NDR-WDR](#) published findings from "The Factory of Fakes", a leak of thousands of files originating from the Social Design Agency that were obtained and first reported by Süddeutsche Zeitung and Delfi Estonia. Experts, journalists, and US intelligence officials [assess](#) the documents to be authentic. The documents revealed further details on how SDA and its founder, Ilya Gambashidze, regularly met with the Russian Presidential Administration and reported on SDA's Doppelgänger operation. According to the documents, SDA's activities include:

- Monitoring Western news sources and social media for ongoing events and evidence of socio-political divisions
- Planning reactive messaging
- Translating these narratives into influence content using writers, designers, editors, and cartoonists
- Posting the resultant content using inauthentic accounts on mainstream social media platforms
- Measuring engagement with delivered content

Attribution

Based on Recorded Future data, leaked SDA documents, the DOJ’s affidavit, and OpenAI’s findings, Insikt Group attributes Operation Undercut activity to the SDA. However, we track this cluster of activity as a likely separate operation from Doppelgänger though working in tandem with existing SDA projects since at least December 2023.

Operation Undercut’s tactics diverge significantly from Doppelgänger’s, which have been previously [described](#) by Insikt Group and [other organizations](#). This is consistent with EU DisinfoLab’s [assessment](#) that similar clusters of influence activity, tracked as [Operation Overload](#) and Matryoshka [1, 2], have diverging TTPs but overlapping infrastructure with Doppelgänger, including Telegram channels and social media accounts, indicating these operations are likely related but distinct from Doppelgänger.

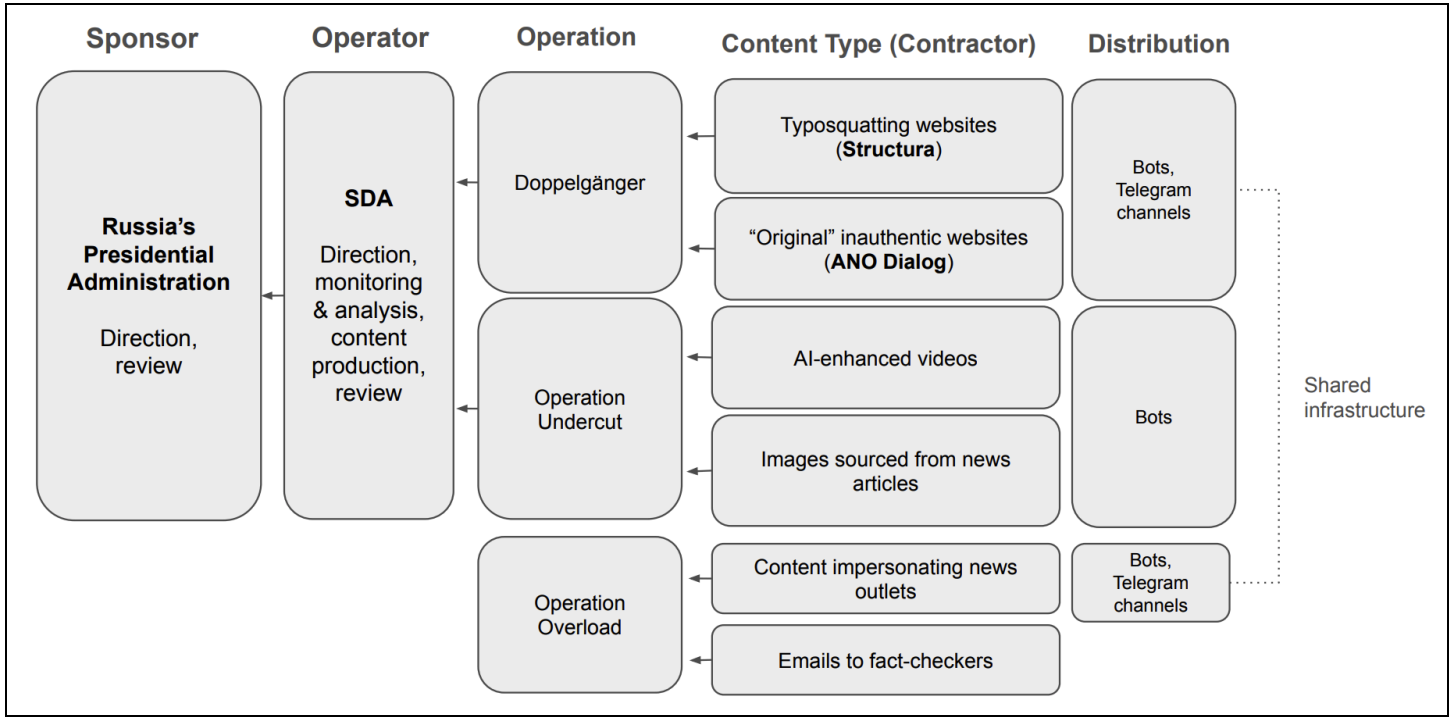


Figure 1: Conceptual framework of suspected influence operations likely conducted by SDA (Source: Recorded Future)

Operation Undercut and Doppelgänger: Likely Separate Operations Conducted by SDA

Operation Undercut is very likely one of several ongoing influence operations managed by SDA. According to the DOJ’s [affidavit](#), SDA is responsible for liaising with the Russian Presidential Administration, strategic planning, monitoring and analysis of Western sources, narrative planning, content production, dissemination, and measuring engagement. Companies contracted by SDA, such as

Structura and ANO Dialog, were likely responsible for creating Doppelgänger's typosquatting domains and "original" websites like Recent Reliable News (RRN), respectively.

Insikt Group has identified the following characteristics indicating that Operation Undercut is a very similar but likely distinct operation from Doppelgänger:

- **Content Production:** Operation Undercut produces a high proportion of unique video and image content not seen on other Doppelgänger assets, which, except for several examples (see [Identical Visual Content](#)), use a different visual identity than known Doppelgänger content.
- **Content Delivery:** Operation Undercut uploads content to social media platforms directly using likely human-operated accounts. Content uploaded by these accounts takes two forms: AI-enhanced videos using a mix of human and AI voiceovers, and images citing or impersonating Western news organizations' coverage of Ukraine. In comparison, Doppelgänger accounts typically post obfuscated links to Doppelgänger's inauthentic websites.
- **Content Amplification:** Doppelgänger used large numbers of automated accounts to boost online engagement. Operation Undercut accounts likely did not receive any such boosting, except for low-volume boosting of 9gag content, which was likely by human-operated accounts rather than bots.
- **Different Accounts:** We did not observe Operation Undercut accounts sharing any links or content attributed to known Doppelgänger websites. Likewise, we did not observe any Doppelgänger accounts promoting content originally posted by Operation Undercut accounts.
- **No Obfuscation:** While Doppelgänger has almost certainly invested significant resources in building and migrating its obfuscation of infrastructure, which includes Keitaro servers and two stages of redirection domains to funnel social media users to its inauthentic websites and measure engagement, Operation Undercut directly uploads content to social media without obfuscating its activities.

However, we also observed the following behavioral and contextual characteristics, which indicate strong similarities between Operation Undercut and Doppelgänger, supporting our attribution of Operation Undercut to SDA:

- **Content Style:** A minority of content posted by Operation Undercut accounts (similar to Doppelgänger content but unique and unused elsewhere in open sources) bears very strong stylistic similarities to images found in the SDA leaks, likely indicating the same content production resources (See [Identical Visual Content](#)).
- **Narrative Continuity:** Operation Undercut's content promotes similar narratives to Doppelgänger assets, both of which correspond to objectives and key performance indicators (KPIs) found in SDA's leaked documents and in planning documents included in the DOJ affidavit (see [Narratives](#)).
- **Target Audiences and Languages:** Operation Undercut and Doppelgänger both uploaded content in Russian, English, French, German, Polish, Turkish, and Hebrew.
- **Platform Manipulation:** Both Operation Undercut and Doppelgänger accounts used trending hashtags in targeted countries in their posts to boost engagement (See [Localized Hashtag Use](#)).

Operation Undercut Is Almost Certainly an SDA-Run Operation

Operation Undercut is almost certainly an influence operation conducted by SDA using a network of social media accounts engaging in coordinated inauthentic behavior (CIB) seeking to achieve influence objectives in support of Russian government interests. Using Insikt Group's Influence Operation Attribution Framework — which is based on a modified version of the North Atlantic Treaty Organization (NATO) Strategic Communications Centre of Excellence [Information Influence Operations \(IIO\) Attribution Framework](#) — the following factors support this attribution:

Behavioral Patterns:

- Network analysis reveals high coordination between accounts sharing identical text content, videos, and images.
- Pattern-of-life (PoL) analysis based on posting times shows that Operation Undercut activity is consistent with Russian office hours and weekdays, indicating that the network is likely either human-operated or simulating human activity.
- Additionally, Operation Undercut accounts did not post on Russian holidays, such as January 7, which is Orthodox Christmas, or May 9, Russia's Victory Day (See [Network Coordination](#)).
- Operation Undercut accounts were posted in specific languages (German, French, Polish, Turkish, and Hebrew) to target audiences similar to Doppelgänger.
- Operation Undercut accounts posted several cartoons (including depictions of targeted leaders and countries and reused fonts) using a visual style identical to cartoons seen in leaked SDA files, indicating that these cartoons were very likely produced by the same artists.
- The volume of unique, original content posted by Operation Undercut accounts shows that the network's operators very likely have access to in-house content creation capabilities, including graphic designers, video editors, and illustrators.
- There are strong similarities between Operation Undercut and Doppelgänger, with the latter being directly tied to the SDA through [leaked SDA documents](#) and a US Department of Justice (DOJ) [affidavit](#).
- In several instances, Operation Undercut accounts promoted influence content produced by the Russian influence network CopyCop (also [tracked](#) as Storm-1516), which is likely funded and directed by Russian intelligence services.

Contextual Evidence:

- Operation Undercut accounts promoted narratives discrediting the US government and its allies, including Ukraine, the UK, France, Germany, Poland, and Türkiye.
- Accounts attempted to manipulate public opinion on tactical developments in the Russian invasion of Ukraine, including Ukraine's Kursk incursion, deterring Western allies from supporting Ukraine via nuclear threats, and discrediting Ukrainian political and military leadership.
- Accounts promoted narratives stoking fears around political violence in the 2024 US elections following assassination attempts on Donald Trump.
- Accounts tried to discredit the 2024 Paris Olympics, including specific sub-narratives promoted by other known Russian operations such as Matryoshka.

Identical Visual Content with Leaked SDA Documents

Insikt Group has observed Operation Undercut uploading original content strongly resembling cartoons found in leaked SDA documents. Operation Undercut accounts posted cartoons with similar caricatures of Zelensky, "Uncle Sam", and Ukraine (personified as a character wearing a traditional kosovorotka shirt), identical fonts, and similar narratives as cartoons found in leaked SDA documents. In addition to being nearly identical to those found in leaked SDA documents, Operation Undercut cartoons have strong visual similarities to cartoons also [uploaded](#) by Doppelgänger's inauthentic websites and accounts, suggesting that one of SDA's cartoon artists is very likely producing visual material for both Doppelgänger and Operation Undercut.



Figure 2: Image posted by Operation Undercut 9gag account (left); image included in leaked SDA documents (right)
(Source: [9gag](#), [Factory of Fakes](#))

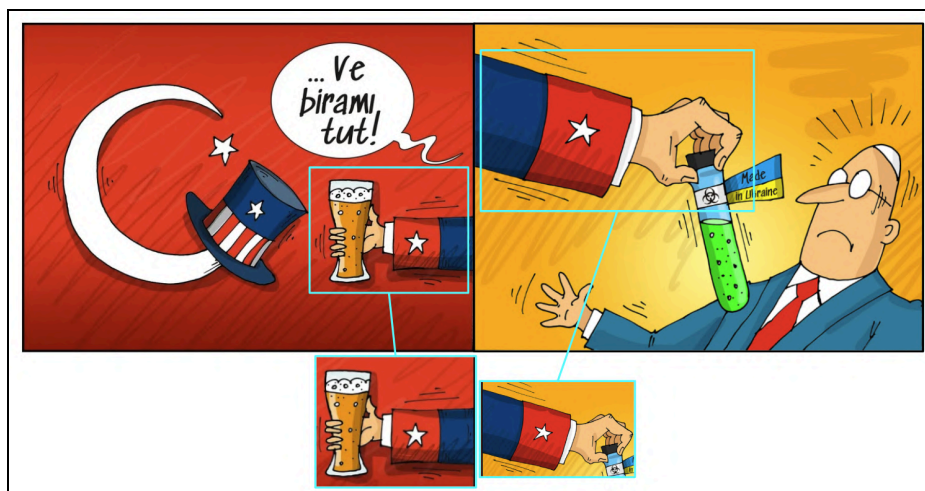


Figure 3: Image posted by Operation Undercut 9gag account (left); image included in leaked SDA documents (right)
(Source: [9gag](#), [Factory of Fakes](#))

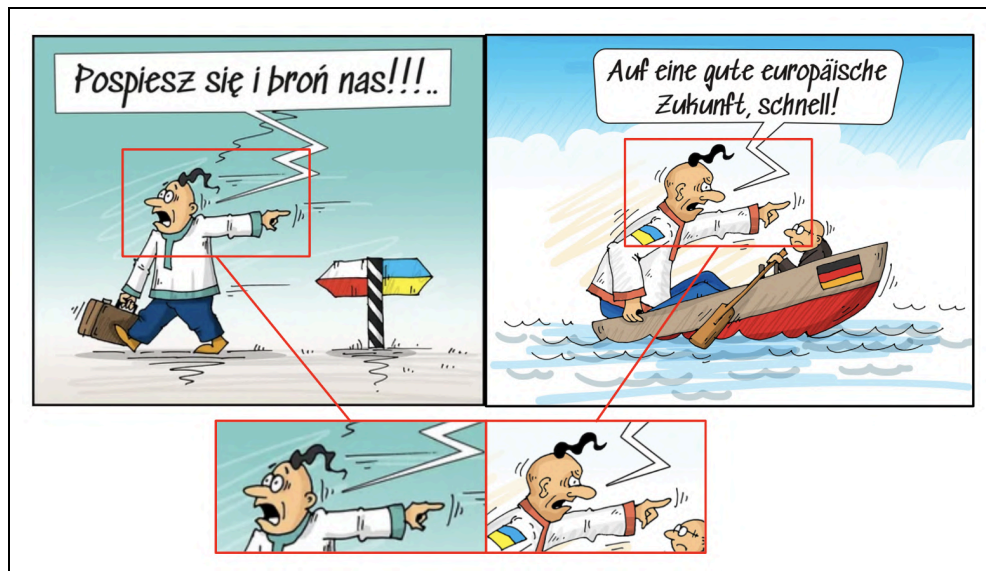


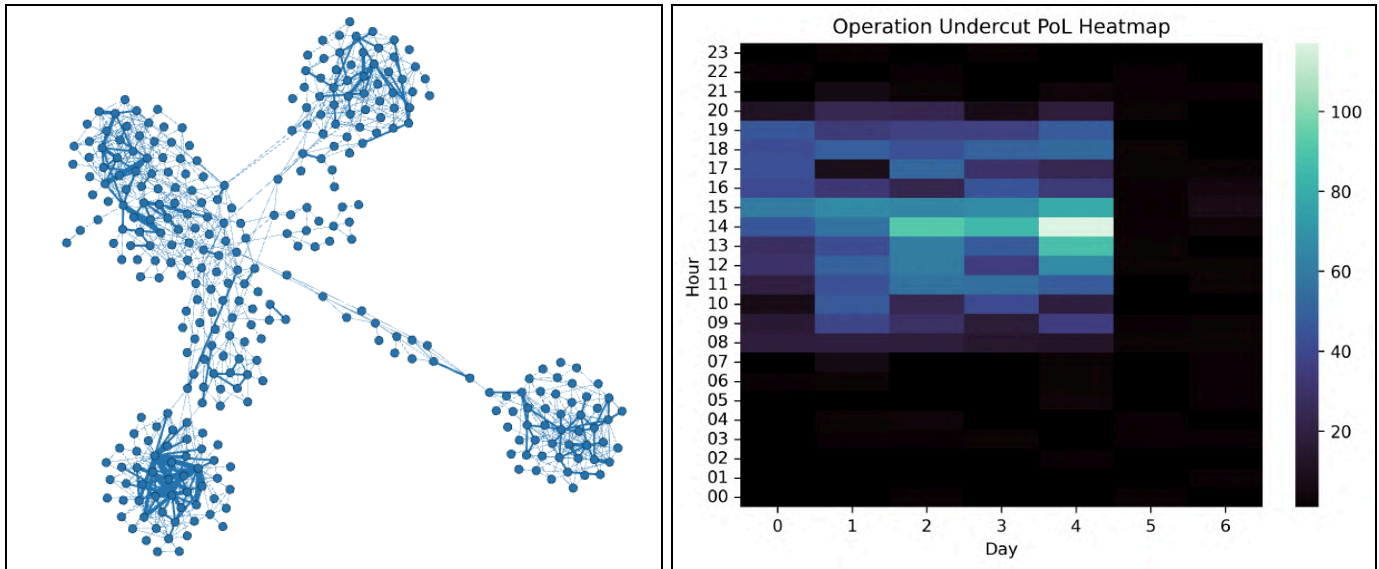
Figure 4: Image posted by Operation Undercut 9gag account (left); image included in leaked SDA documents (right)
(Source: [9gag](#), [Factory of Fakes](#))

Operation Undercut accounts posting these cartoons also posted [AI-enhanced videos](#) on 9gag, including identical ones observed on other social media platforms. For example, an account named "Alisha Benjamin" [posted](#) both the Zelensky caricature in **Figure 2** and several AI-enhanced videos unique to Operation Undercut, such as a video titled "The head of the Ukrainian army was dismissed for incompetence", using an identical format as other videos described in this report. An account named "Caleb Tucker" [posted](#) both the Uncle Sam caricature in **Figure 3** and an AI-enhanced video encouraging Germany to leave the EU and NATO. An account named "Carrie Thompson" [posted](#) both the caricature of Ukraine in **Figure 4** and an AI-enhanced video named "Israel's future can't depend on an ally that's more interested in politics than our safety!"

Network Coordination

Insikt Group identified Operation Undercut accounts by pivoting on identical content posted across multiple accounts ("cypypasta"). Of the accounts analyzed by Recorded Future, 10% of accounts posted in more than one language.

Pattern-of-life (PoL) analysis of Operation Undercut posting behaviors reveals that the network follows a regular working schedule, with most posts being made on typical work days (Monday through Friday) between 9 AM GMT and 7 PM GMT. This behavior demonstrates a high degree of coordination across accounts and likely points towards either human operators or automated accounts simulating human activity periods. As noted above, accounts did not post on Russian holidays, such as January 7, which is Orthodox Christmas, or May 9, Russia's Victory Day, providing more indications the network is very likely operated from Russia, further supporting our almost certain attribution of Operation Undercut to the SDA.



Figures 5 and 6: Social network analysis (left) and heat map (right) of Operation Undercut accounts, Monday (0) to Sunday (6), GMT (Source: Recorded Future)

Narratives

Insikt Group has observed similarities in the narratives amplified by Operation Undercut with narratives amplified by Doppelgänger. Through AI-enhanced videos and images quoting or impersonating Western media outlets, accounts have focused on the following narratives between July and September 2024:

- Undermining Western military support for Ukraine, including by discrediting Ukrainian political leadership
- Exacerbating tensions between Western allies over the Israel-Gaza conflict and highlighting domestic protest movements in the US and UK
- Escalating internal EU tensions by supporting the rise of far-right parties in France and Germany in addition to exploiting tensions between EU member states, Ukraine, and Brussels
- Framing global conflict as being dependent on the result of the 2024 US elections and exacerbating domestic fears over political violence and assassination attempts
- Criticizing the 2024 Paris Olympics

Insikt Group identified very little organic engagement with Operation Undercut accounts. As highlighted in OpenAI's report, Operation Undercut's attempts to boost engagement on platforms like 9gag resulted in users identifying the accounts as inauthentic. Despite our broader scope of investigation and discovery of over 500 accounts, we assess that Operation Undercut's activities can be classified as Category 2 on the Brookings Institution's [Breakout Scale](#), reflecting the network's cross-platform activity without significant audience engagement.

Undermining Western Support to Ukraine and Ukrainian Leadership

The majority of content published by Operation Undercut seeks to undermine Western public support for military aid to Ukraine, by attempting to:

- Undermine support for allowing Ukraine to strike targets in Russia
- Accuse Ukraine of sponsoring the Crocus City Hall attacks and financing “terrorist” anti-Wagner forces in Mali and Niger
- Promote Russian forces’ progress in Kursk and Crimea
- Disparage US leadership for allegedly pressuring Ukraine to pursue a peace deal
- Question the effectiveness of Western military equipment in Ukraine
- Discredit President Volodymyr Zelensky and broader Ukrainian political and military leadership
- Promote Russia’s new nuclear doctrine, which seeks to dissuade Ukrainian long-range strikes targeting Moscow

As above, Insikt Group identified a number of Operation Undercut videos seeking to discredit Ukrainian military and political leadership with similar narratives, with at least thirteen Ukrainian officials being accused of corruption for using foreign military aid and government funding to purchase luxury villas in Europe and the Caribbean. These videos were mostly produced in French and German, indicating that these countries were likely the target audiences for undermining domestic support for aid to Ukraine in these countries.

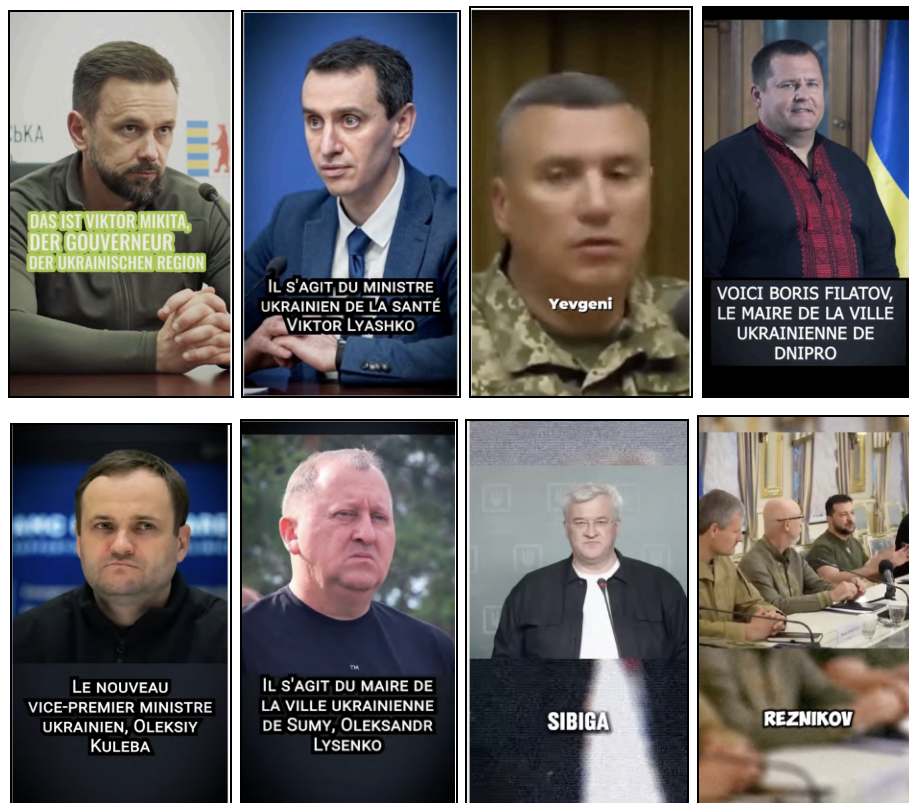


Figure 7: Ukrainian military and political figures targeted by Operation Undercut content (Source: 9gag [1](#), [2](#), [3](#), [4](#), [5](#), [6](#), [7](#), [8](#))

Between August and September 2024, Operation Undercut accounts posted two videos in support of Russia's evolving nuclear doctrine in relation to Ukraine. The first quotes an August 2, 2024, TASS article claiming that the Russian drone manufacturer CBDR developed a first-person view (FPV) drone with nuclear safety capabilities as part of the "[Khrust](#)" radiation monitoring project.¹ The second covers Vladimir Putin's September 25, 2024, announcement that Russia was [revising](#) its nuclear doctrine to permit retaliatory strikes in the event of conventional strikes against Moscow, even by non-nuclear states such as Ukraine.

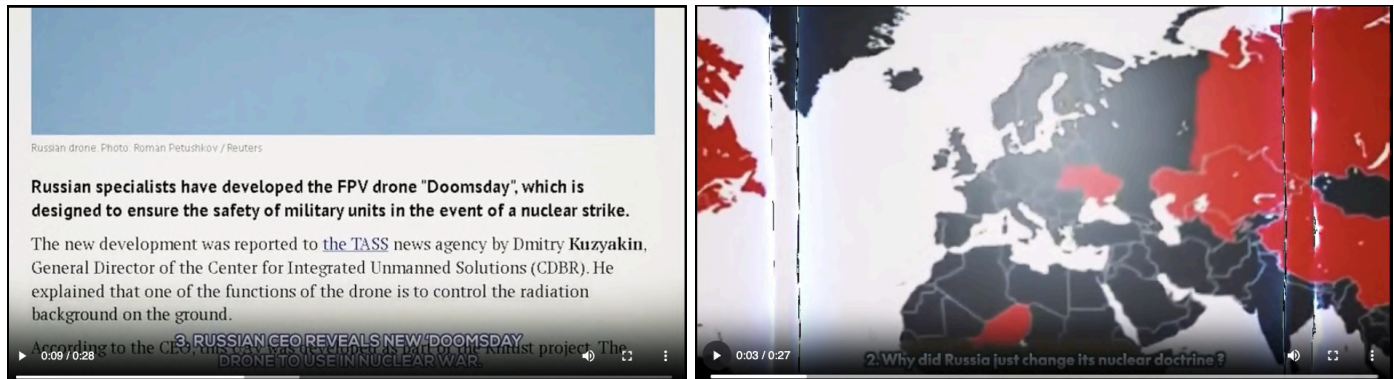


Figure 8: Operation Undercut content promoting Russia's nuclear doctrine (Source: Social Media)

Exacerbating Tensions over the Israel-Gaza Conflict

According to the DOJ's September 4, 2024, [affidavit](#), SDA chose to report on the Israel-Gaza conflict both to exacerbate tensions between Israel and Western allies and to influence the 2024 US elections by influencing "associated religious and ethnic groups" in the US. Operation Undercut pursued this goal by [accusing](#) Israel of [bombing](#) a humanitarian zone in Al-Mawasi; accusing UK, US, and Turkish intelligence agencies of supporting Hamas; and questioning Western military aid to Israel. The network also posted content likely attempting to exacerbate increasing domestic tensions by posting about protests in Western countries, claiming, for example, that pro-Palestinian protestors in New York City were spotted carrying Hamas flags and covering a pro-Palestinian protest in London demanding "an end to arms sales to Israel".

¹ [https://tass\[.\]com/defense/1824845](https://tass[.]com/defense/1824845)



Figure 9: Operation Undercut content about the Israel-Gaza conflict (Source: [9gag](#), Social Media)

Escalating Internal EU Tensions

The EU, its member states, and European audiences are persistent targets of Doppelgänger and Operation Undercut, likely as part of the SDA's "International Conflict Incitement", which, according to the DOJ's affidavit, [aims](#) to "escalate internal tensions in the countries allied with the United States in order to promote the interests of the Russian Federation on the international arena". Social media accounts affiliated with Operation Undercut have posted content supporting Europe's far-right political parties and exploiting tensions between EU member states, Ukraine, and Brussels on topics like EU-Russia relations and introducing additional sanctions on Russia.

Leaked documents [show](#) that Doppelgänger operators working for SDA had specific key performance indicators (KPIs) based on polling data related to far-right European parties National Rally (France) and AfD (Germany) ahead of the 2024 EU elections. We observed continued posting of content in support of these KPIs by Operation Undercut accounts until at least September 2024, demonstrating enduring support for these parties, even after the European elections.

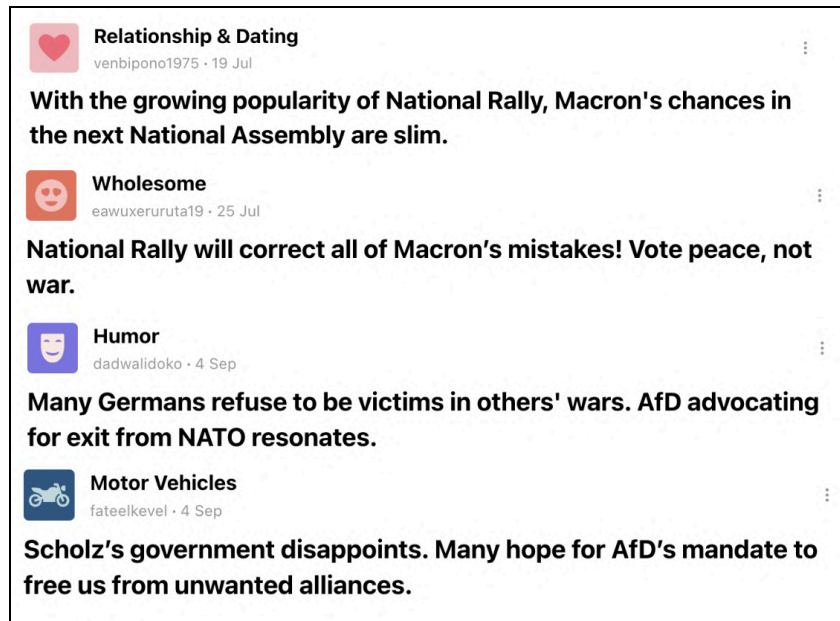


Figure 10: Operation Undercut posts supporting National Rally and AfD (Source: 9gag [1](#), [2](#), [3](#), [4](#))

Operation Undercut content also attempted to exploit tensions between EU member states and Brussels. For example, Polish-language content labeled EU Commission President Ursula von der Leyen a “puppet” of the German government shortly following her re-election on July 18, 2024, and accused her of influencing Polish policy, claiming that Poland Prime Minister Donald Tusk and von der Leyen’s ideas had “destroyed the Polish economy”.



Figure 11: Operation Undercut content targeting Ursula von der Leyen (Source: Social Media)

Additionally, content published by Operation Undercut attempts to exacerbate existing tensions between EU members and Ukraine. Accounts posted content summarizing legitimate statements issued by senior ministers from Germany, Poland, Hungary, Slovenia, and Slovakia, attempting to frame the statements as EU countries pressuring Brussels to repair relations with Russia, veto further sanctions, and block Ukraine’s accession path to the EU. Accounts also used Ukraine’s alleged responsibility (according to Russia) for sabotaging the Nord Stream pipeline as a speculative reason for increased tensions.

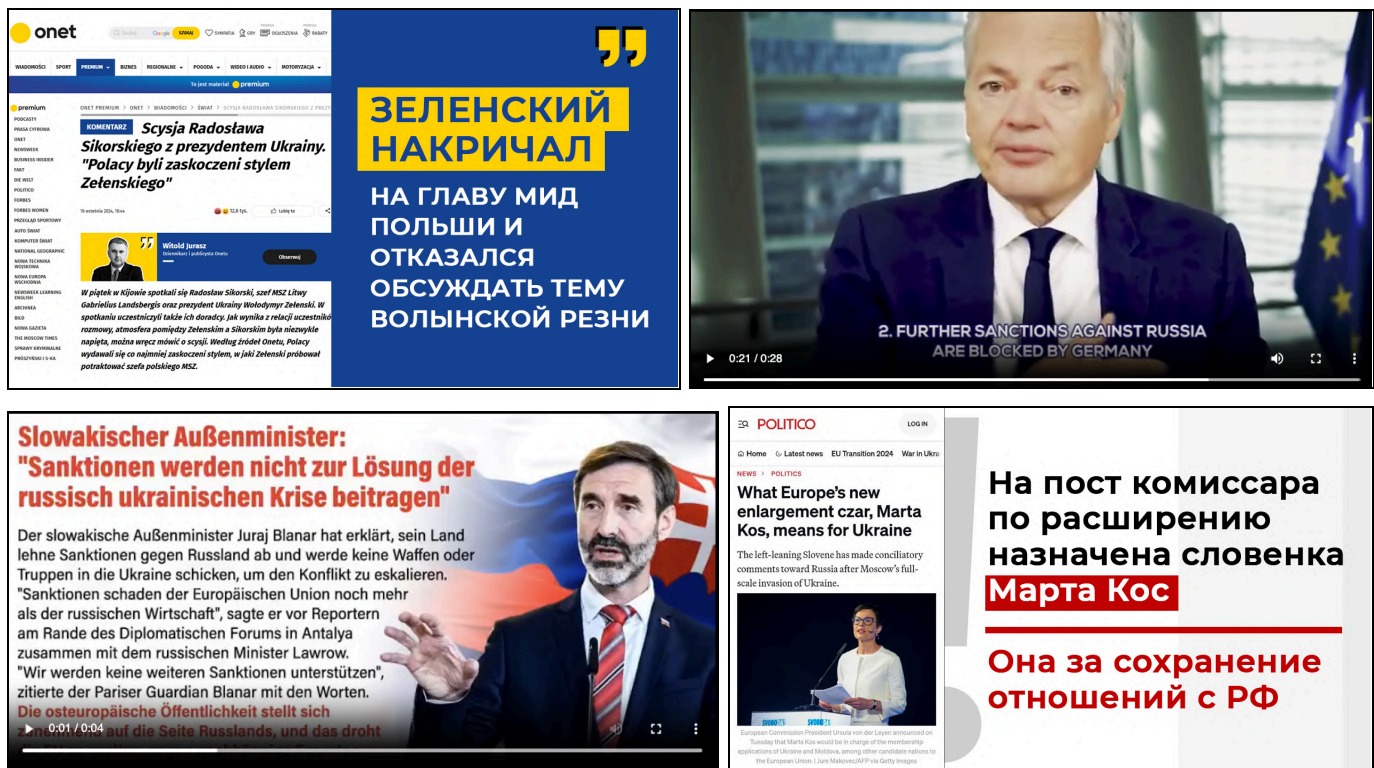


Figure 12: Operation Undercut content seeking to exploit tensions between EU member states, Ukraine, and Brussels (Source: Social Media)

Framing Global and Domestic Conflict as Dependent on the 2024 US Elections

Operation Undercut accounts also amplified influence content related to the 2024 US elections, with the majority of content focused on the uncertainty of continued US military aid to Ukraine, suggesting it was dependent on the results of the election. They claimed, for example, that military aid remains “a popular tool” for US leaders and is “likely to play a key role in defense policy after this year’s election”, and that “the outlook of the flow of US aid to Ukraine, which is highly uncertain owing to the coming US presidential election, could have an important impact on the progress of the war”, using the imagery of a roulette table to represent the uncertainty of US aid to Ukraine.



Figure 13: Operation Undercut content suggesting military aid to Ukraine was dependent on 2024 US election results
(Source: Social Media)

Other videos were more direct in their attempts to undermine President Joe Biden and Vice President Kamala Harris. For example, one video covered the June 27, 2024, presidential debate between President Biden and former President Trump and [claimed](#) that “Hollywood sponsors” were “offended by the [Biden] campaign’s claims that the President won the debate”. Another video attempted to support claims that Vice President Harris was not “deeply involved in attempts to develop foreign policy in general, or Ukraine-Russia in particular”.



Figure 14: Operation Undercut content undermining President Biden and Vice President Harris
(Source: [9gag](#), Social Media)

We also identified limited evidence of Operation Undercut accounts promoting narratives about contentious domestic issues in the US election. While we did not find any exact replicas of this cartoon in leaked SDA documents, Insikt Group identified [one cartoon](#) posted by an account affiliated with Operation Undercut strongly resembling the style of cartoons included in the document leaks (including similar fonts and character styles) implying that the Democratic Party would encourage illegal immigration in the event of electoral victory.



Figure 15: Cartoon posted by an account affiliated with Operation Undercut closely resembling leaked SDA materials
(Source: [9gag](#))

Operation Undercut also attempted to exacerbate fears of growing political violence in the US following assassination attempts on former President Trump. One video covered vice-presidential candidate JD Vance's [comments](#) that "no one has tried to kill Kamala Harris", while another highlighted [claimed](#) links between assassination attempt suspect Ryan Routh and the Ukrainian military. We also observed content covering the assassination attempts in languages other than English (such as French, **Figure 16**), indicating that one of Operation Undercut's objectives is also to shape international perceptions of the integrity of the US elections and attempt to paint Ukraine as being responsible for the second assassination attempt against former President Trump.

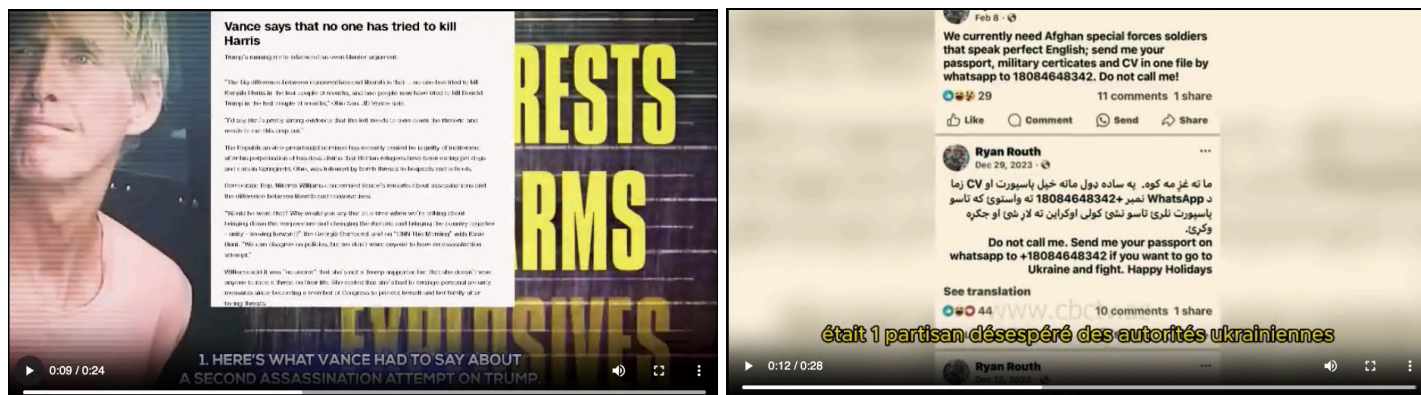


Figure 16: Operation Undercut content undermining President Biden and Vice President Harris
(Source: Social Media)

Criticizing the 2024 Paris Olympics

To a more limited extent, Operation Undercut accounts also promoted polarizing narratives targeting the 2024 Olympic Games, which was a [broader target](#) for Russian influence operations. In addition to accounts amplifying content from other Russian actors, such as a CopyCop video portraying a member of Hamas threatening the Olympics (see [Amplification of CopyCop Content](#)), the network also posted original content in reaction to major news stories during the Olympics. This included criticizing the 2024 Paris Olympics opening ceremony, calling it “extremely disrespectful to Christians”, highlighting reports that the Seine River was not clean enough for triathletes, and amplifying transphobic narratives targeting Algerian boxer Imane Khelif. Several German-language videos also claimed that, in light of “terrorist threats” to the Olympics, “3 million tickets have gone unsold”, a narrative French disinformation agency VIGINUM has seen being [promoted](#) mainly by Operation Overload/Matryoshka.

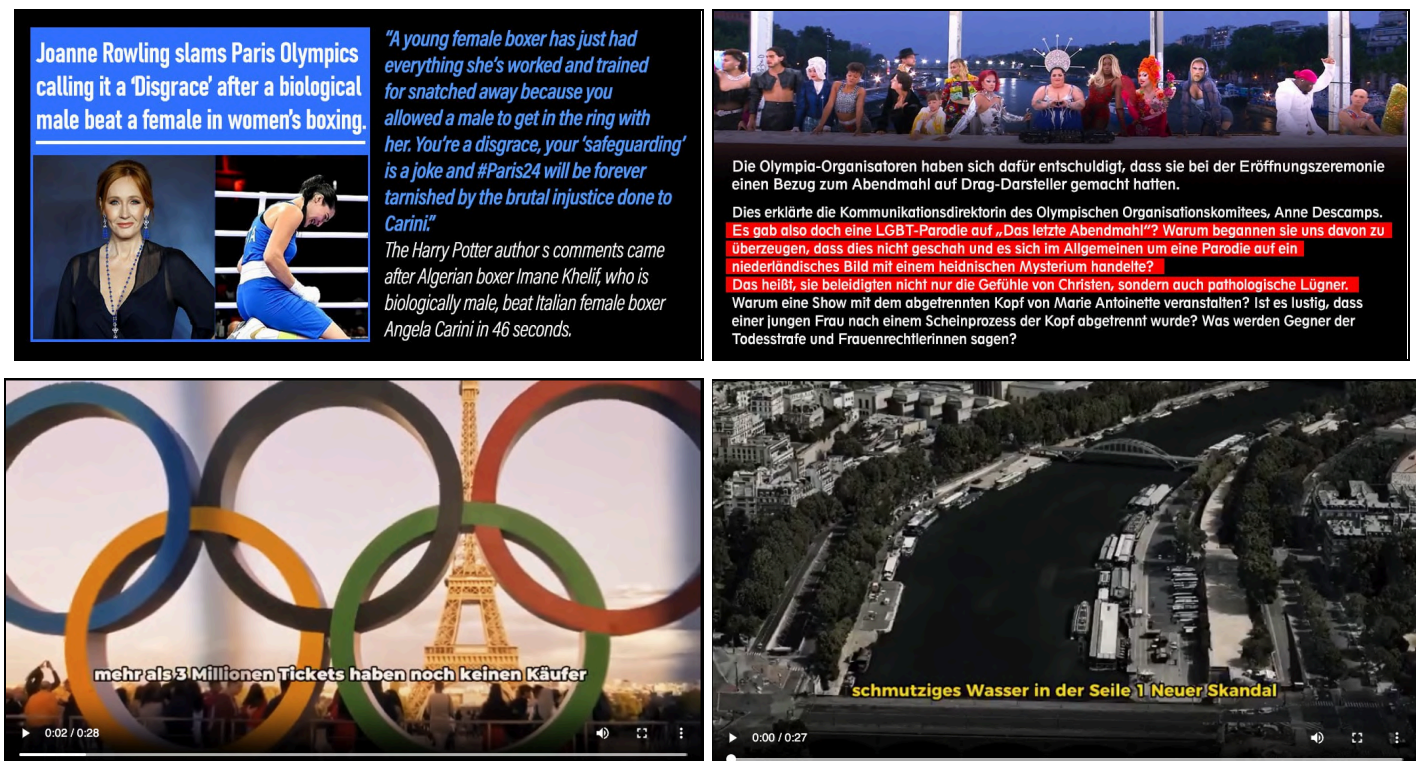


Figure 17: Operation Undercut content targeting the Olympics (Source: Social Media)

Tactics, Techniques, and Procedures (TTPs)

Operation Undercut uses video content with AI-generated voiceovers and images that reference real articles by Western media outlets but take fragments of information, such as quotes perceived as negative towards Ukraine, out of context and deceptively repackage the information to support its influence objectives — a practice commonly referred to as “cherry-picking”. Social media posts containing Operation Undercut content often abuse trending hashtags in target audience countries at the time of upload to maximize engagement, in addition to posting content to non-mainstream social media platforms like 9gag. For the first time, we have also observed an almost certainly SDA-affiliated influence operation posting unique content originally produced by CopyCop, indicating a level of collaboration or awareness between the two networks. These tactics are also similar to those used by [Operation Overload](#), which [principally relies](#) on AI-generated content and media impersonations to give its content credibility and spread similar narratives.

AI-Enhanced Video Content

While some Operation Undercut videos use human narrators, a significant number of these videos use AI-generated voiceovers in Russian, English, German, Polish, French, and Turkish. We also identified one post using a title in [Hebrew](#) but with a Russian-language video. Out of a sample of 400 accounts, we identified 1,190 videos with 233 unique transcripts. Operation Undercut’s operators are likely using multiple commercial AI services to generate voiceovers, [including](#) ElevenLabs. We also identified a minority of English- and Russian-language videos using human voiceovers. English-language videos with a human voice typically contained a discernible Russian accent.

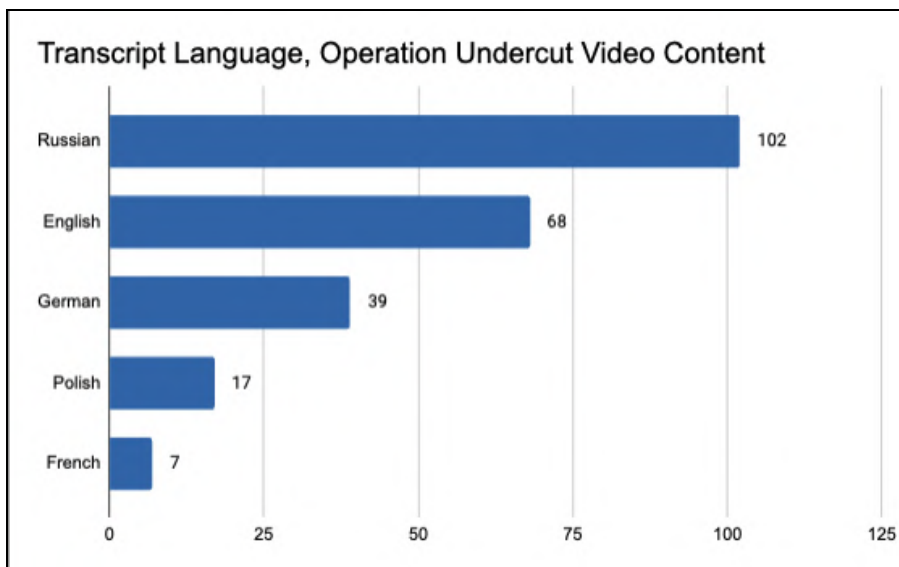
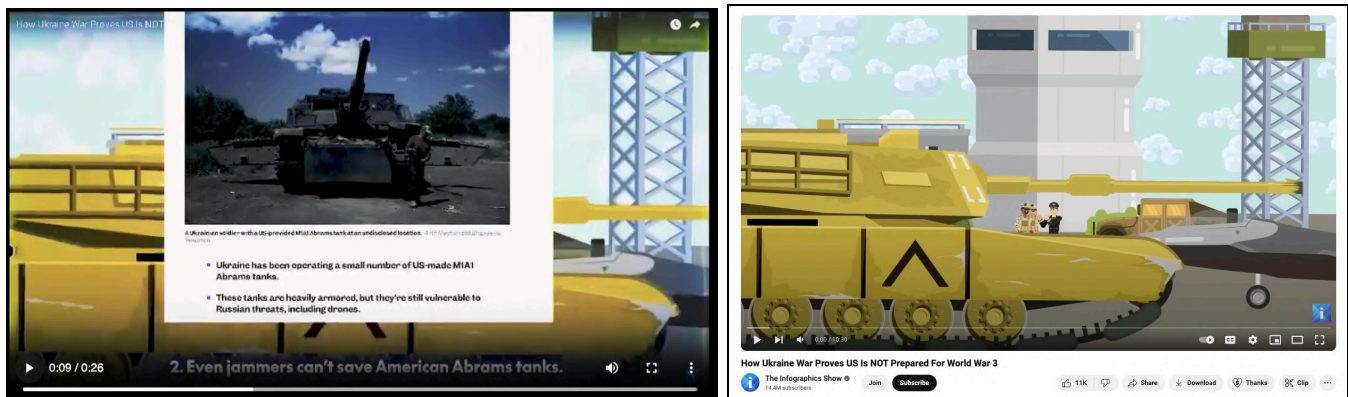


Figure 18: Transcript language, Operation Undercut video content (Source: Recorded Future)

In some instances, we observed Operation Undercut accounts publishing videos that were likely screen-recorded from publicly available content such as YouTube videos. In one case, we identified an Operation Undercut video attempting to question the effectiveness of M1 Abrams tanks delivered to Ukraine using footage from a video originally [published](#) by The Infographics Show, a YouTube channel (**Figure 20**). The video included an overlay of the YouTube video being played, an advertisement preceding the video as typically shown on the video platform, and a widget from screen-recording software.



Figures 19 and 20: Operation Undercut video (left) using footage from a legitimate YouTube channel (right)
(Source: Social Media, [YouTube](#))

Impersonating and Framing Legitimate Media Content

In addition to publishing AI-enhanced videos, Operation Undercut accounts also typically publish image content containing a screenshot of an article by a legitimate media outlet, a translated quote from the article, and the media outlet's logo or text visuals resembling the media outlet's brand. In Operation Undercut account posts featuring quotes copied from authentic media articles, the quotes were often taken out of context and highlighted to show criticism of Ukraine and its Western allies. Insikt Group has identified such content using articles from Politico, The New York Times, Le Monde, Forbes, CNN, Financial Times, The Wall Street Journal, Europe1, Responsible Statecraft, Le Figaro, Euro News, and Die Freie Welt. Insikt Group has not observed any instances of these images being used outside of Operation Undercut accounts, indicating that Operation Undercut content is almost certainly produced organically by the network's operators rather than being repurposed from external sources.

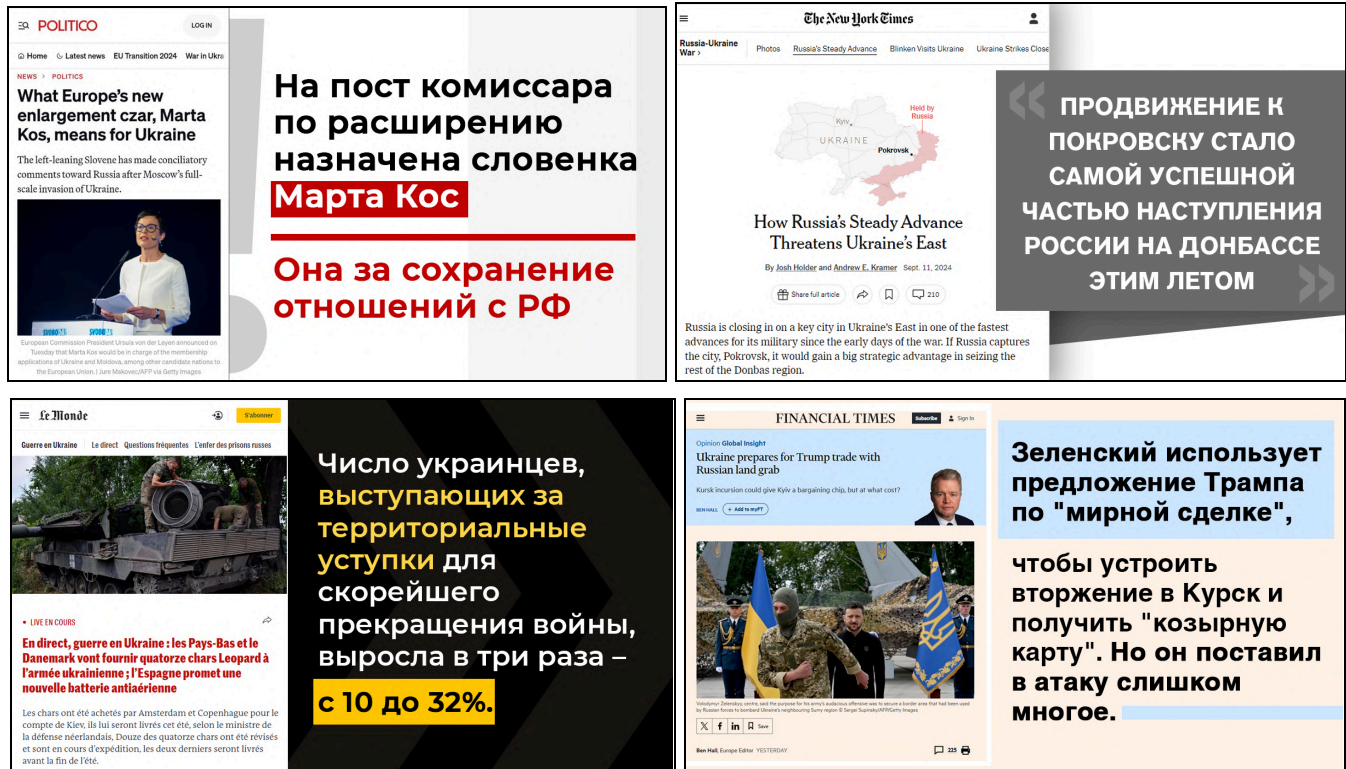


Figure 21: Operation Undercut content repurposing articles from legitimate media outlets
(Source: Social Media)

Localized Hashtag Use

Similarly to previously observed Doppelgänger activity, Insikt Group observed Operation Undercut using trending hashtags in targeted countries and languages to amplify its content, very likely looking to target specific audiences in Ukraine, the US, the UK, and Europe. These target audiences (depicted below) strongly resemble those targeted by Doppelgänger.

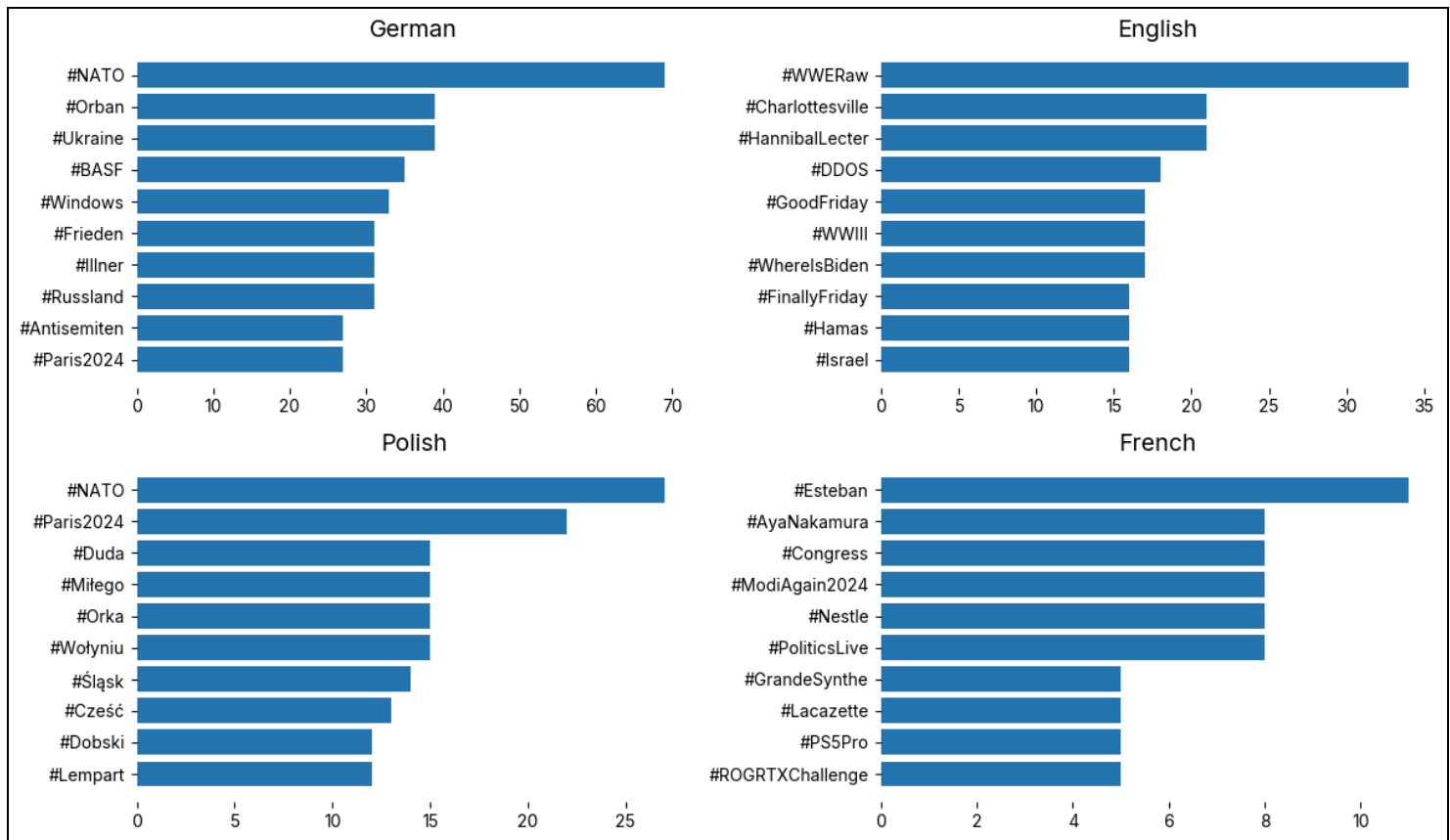


Figure 22: Top hashtags used by Operation Undercut accounts in each language (Source: Recorded Future)

Alternate Social Media Platforms

Insikt Group identified a network of accounts posting Operation Undercut content on alternate social media platforms, including [9gag](#) and [americasbestpics\[.\]com](#). Most 9gag accounts identified by Insikt Group were created on June 12, 2024, two weeks after the aforementioned OpenAI [report](#) on the activity. Accounts primarily posted AI-enhanced video content using the same format as accounts previously described in this report but also posted caricatures and memes, consistent with typical content on 9gag. As noted by OpenAI, Operation Undercut accounts on 9gag upvoted and posted comments on each other's posts to boost engagement metrics. However, these posts obtained very little organic engagement, with many 9gag users identifying the accounts as inauthentic and Russia-affiliated.

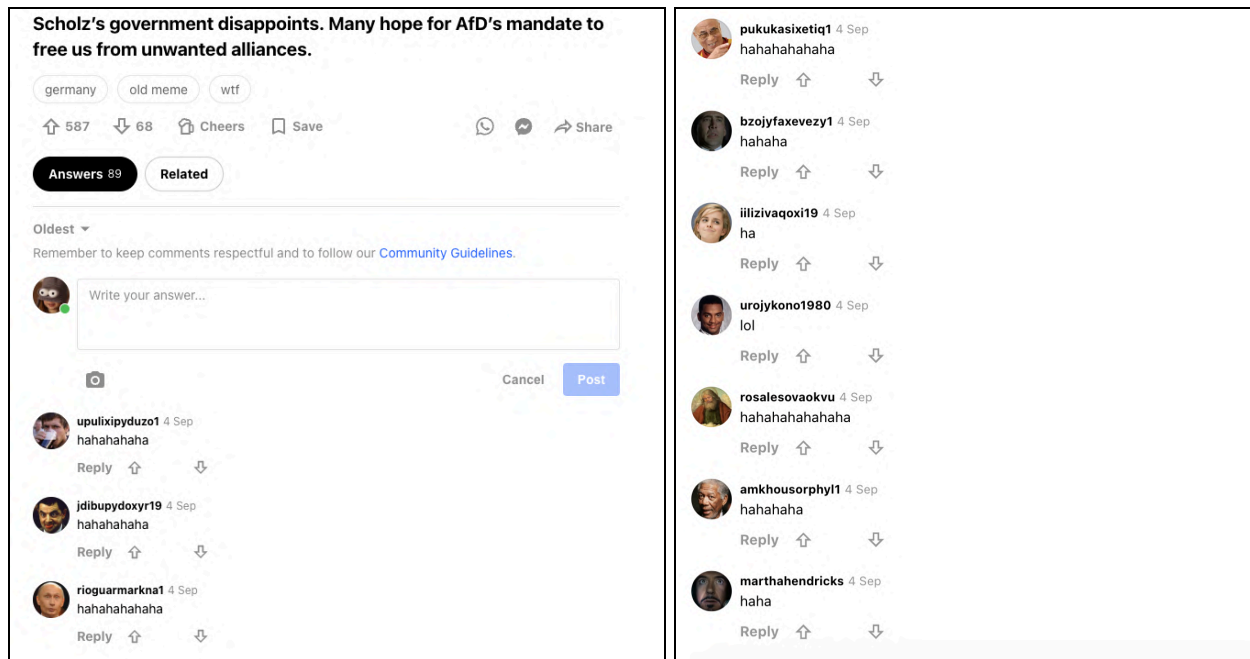


Figure 23: Comments posted by Operation Undercut accounts on other accounts' posts (Source: [9gag](#))

Amplification of CopyCop Content

In several instances, Insikt Group identified Operation Undercut content amplifying content from CopyCop (also [tracked](#) as Storm-1516), a Russian influence network [attributed](#) to John Mark Dougan and, [according](#) to Microsoft and leaked documents [seen](#) by the Washington Post, sponsored by Alexander Dugin's Centre for Geopolitical Expertise (CGE) and the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) Unit 29155. CopyCop content reuploaded by Operation Undercut included a deepfake video of an alleged Hamas member threatening the 2024 Paris Olympics and an article [accusing](#) Zelensky of purchasing an Italian villa during the 2024 G7 summit.

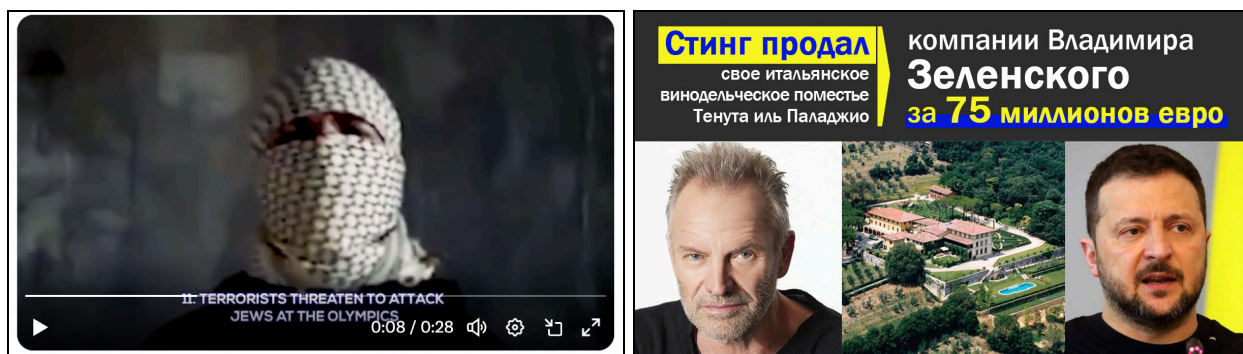


Figure 24: Operation Undercut posting content originally developed by CopyCop (Source: Social media)

This is the [second](#) known instance of an SDA-affiliated influence operation amplifying CopyCop content. However, we are unable to determine whether this is the result of internal coordination between the CGE, GRU, and SDA, or if SDA has opportunistically capitalized on media attention to both narratives to perpetuate its narratives.

Mitigations

- News organizations should track content from known influence threat actors who are likely abusing their brand. Such abuse increases reputational risks and erodes consumer trust, potentially deterring advertisers and inflicting financial harm on the impersonated organizations.
- Political leaders and government officials from countries providing support to Ukraine should continue monitoring for content attempting to discredit them in order to identify and counter emerging narratives.
- Public and news organizations can use [Recorded Future Brand Intelligence](#) to track and combat typosquatting domains and infringing content on similar domains, which can harm a news organization's reputation.
- Clients can use the Recorded Future Intelligence Cloud to track Operation Undercut activity and Recorded Future AI to summarize and track emerging narratives.

Outlook

The SDA will almost certainly continue conducting multiple influence operations, including Operation Undercut, as it simultaneously likely seeks to rebuild Doppelgänger's obfuscation infrastructure and continue using known content delivery and amplification tactics. Russia's Presidential Administration will almost certainly continue to task the SDA with conducting influence operations that support Russia's broader geopolitical goals. As such, we expect SDA's influence operations to continue to target Ukrainian leadership, attempt to shape international public opinion on Ukraine, and exploit conflicts and events such as elections, major sporting events, and international news to reinforce narratives undermining support for Ukraine.

Our investigative process, which incorporates data from the Recorded Future Intelligence Cloud, US government indictments, leaked documents shared by journalists, and previous reporting by other researchers, highlights the current benefits and ongoing need for a collaborative approach across industry, government, and civil society to disrupt large-scale influence operations conducting destabilizing activities. Transparently documenting and exposing such operations has very likely imposed costs on organizations such as the SDA, including forcing operators to conduct infrastructure migration, highlighting the role of foreign companies in influence operations (leading to international sanctions), and frustrating these entities' sponsors.

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