THREAT ANALYSIS

RUSSIA

Recorded Future®

By Insikt Group®

February 13, 2025

Stimmen aus Moskau:
Russian Influence Operations Target German Elections

The February 23, 2025, German elections are a target of Russian influence operations. As of mid-February, these operations have very likely not meaningfully altered voter behavior or public opinion.

These operations almost certainly aim to inflame German sociopolitical divisions, spread manipulated content, foster anti-US and EU sentiment, and weaken NATO unity in line with Kremlin objectives.

Despite very likely having limited voter impact to date, the persistence and evolving tactics of these campaigns elevate the risk of a breakout influence event, as seen in a recent anti-USAID video.

Executive Summary

The German federal elections, scheduled for February 23, 2025, are the target of malign influence operations linked to Russia and Russia-based actors. As of mid-February 2025, Insikt Group assesses that, despite their persistence, these efforts have very likely not meaningfully altered voter behavior or shaped public opinion in a manner advantageous to Russia's broader geopolitical interests, consistent with assessments of Russian meddling attempts in previous German election cycles.

The influence operations and corresponding networks tracked in this report — Doppelgänger, Operation Overload, CopyCop, Operation Undercut, and the Russia-based Foundation to Battle Injustice — are longstanding and at least partially Kremlin-funded. These operations almost certainly seek to incite and escalate German domestic sociopolitical conflicts, pollute the German information space by introducing manipulated content, foster criticism of the United States (US) and European Union (EU) and European integration, and undermine North Atlantic Treaty Organization (NATO) cohesion in line with the Kremlin's strategic objectives.

The 2025 German election cycle marks a period of evolution for several of these operations, while core narratives remain unchanged. For example, Doppelgänger and Operation Overload have expanded beyond mainstream social media to Bluesky Social (Bluesky), in an attempt to capture migrating audiences. Doppelgänger and CopyCop have launched new brands and websites to project influence and reinforce messaging in the face of intensified scrutiny of their operations. Operation Overload continues to use artificial intelligence (AI)-based tools, including the use of AI-enabled voice cloning technology to create audio deepfakes, while both Operation Overload and Operation Undercut pose as real news organizations to increase their credibility.

Despite limited evidence that these operations have meaningfully influenced voter behavior, they still pose broader risks to media integrity and public trust. Narratives undermining election security or integrity could reduce voter turnout, while media engagement with inauthentic content — rather than exposing the tactics behind it — may amplify malign messaging. Regarding Operation Overload specifically, we continue to assess that the potential for significant breakout does exist, as evidenced in the viral spread of a recent video attributed to this network that disparaged the United States Agency for International Development (USAID) in social media. To mitigate these risks, media entities, the public sector, and researchers should continue monitoring known influence networks while limiting engagement with operations such as Doppelgänger, Operation Overload, and Operation Undercut. Impersonated organizations should engage takedown services for malicious domains, collaborate with platform trust and safety teams, and proactively detect brand abuse tactics like typosquatting and logo manipulation.

Key Findings

- The German federal elections are the target of malign influence operations attributed to Russia and Russia-based actors.
- Russia-attributed influence operations have promoted and will very likely continue to support German political parties Russia views as beneficial to its own geopolitical interests, particularly Alternative für Deutschland (AfD).
- Doppelgänger is very likely exerting influence through at least seven new inauthentic news brands, in addition to the operation's persistent media impersonation activities, to exacerbate political fissures and inflame political discourse surrounding European integration, immigration, and economic matters.
- Operation Overload's media impersonations aim to sow distrust among German citizens toward the safety and integrity of voting, attack the characters of key political leaders, and present Germany as a rising hotbed of antisemitism and extremism.
- Insikt Group detected at least 94 new inauthentic websites — whose creation began in November 2024 after the announcement of upcoming snap elections — that we attribute to CopyCop impersonating German-language news websites.
- Following Insikt Group's November 2024 investigation into Operation Undercut, we have observed the network continuing to post German-language content supporting AfD and undermining German Chancellor Olaf Scholz.
- The Foundation to Battle Injustice very likely seeks to undermine the reputations of German political leaders while promoting political platforms aligned with Russian interests through inauthentic investigative articles.

New Doppelgänger "Brands" Target Key German Election Issues

Insikt Group has detected at least eight new websites acting as original news brands, in addition to continued media impersonation with social media promotion, which we attribute to Doppelgänger, a longstanding Russian influence operation. Doppelgänger is very likely positioning these newly established websites — previously not linked to the network — to sustain its influence operations targeting European political leadership and to exacerbate political fissures surrounding European integration, immigration, economic matters, and more. Throughout 2024, researchers, government entities, and technology companies continued exposing Doppelgänger's activities across Europe and North America, leading to a US Department of Justice indictment against its operators at the Social Design Agency (SDA), international sanctions on SDA and affiliated entities, and at least partial — though often temporary — disruptions to its operations through takedowns and seizures. In response, SDA typically attempted to reestablish its operations within hours to days by deploying new infrastructure.

While Doppelgänger is best known for the direct impersonation of legitimate Western media organizations, the influence operation has also managed a multitude of its own original news website "brands", each targeting a specific country (such as Germany), with content directly tailored to the key domestic and foreign policy issues of that target audience, such as immigration policy, Germany's

ongoing socio-economic challenges, and questions of Germany's place as Europe's leader (as seen in **Figure 1**). Insikt Group has observed Doppelgänger abandoning several of its "legacy" brand websites with attempts to establish new brands, including multiple websites specific to German politics, likely due to a combination of repeated discovery and disruption of several of these websites.

While we continue to observe Doppelgänger evolve its tactics and attempt to evade defenders, its ability to meaningfully impact public discourse very likely remains limited. Despite continued efforts to expand its network, Doppelgänger remains constrained by low levels of engagement, with minimal views and interactions across its newly launched domains and social media brands.

Using New Infrastructure to Deliver Old Themes

Since October 2024, Insikt Group has tracked a series of new domain registrations, discovering web page infrastructure that overlaps with previously attributed Doppelgänger-controlled domains. As of February 2025, Doppelgänger has registered ten domains that include eight new websites and two "parked" domains. The active domains reflect seven news brands that target German-speaking audiences:

```
herzheim[.]org
kriminalradar[.]com
militarblatt[.]net
ostlicherwind[.]com
stolzvolk[.]ac
stolzvolk[.]org (currently offline)
tageswirtschaft[.]org
weltwahl[.]com (currently offline)
detechplus[.]com (parked)
sportbericht[.]net (parked)
```

***Figure 1**: New Doppelgänger domains specific to Germany and German-speaking audiences (Source: Recorded Future)*

***Figure 2**: The seven new Doppelgänger brands targeting Germany and German-speaking audiences (Source: Recorded Future)*

Each of the active websites uses distinct IP addresses, listed below, with the exception of *weltwahl[.]com* and *stolzvolk[.]org*, which both share 15.197.130[.]221. Administrators of these domains use web hosting provider resources provided by Hosting Concepts B.V. (d/b/a Registrar.eu), QHoster, NameSilo, Namecheap, or Vicetemple. Stolzvolk's newest domain, *stolzvolk[.]ac*, uses web hosting services provided by Ultahost, Inc.

IP Address	ASN	Organization Name
15.197.130[.]221	AS16509	Amazon Technologies, Inc.
162.255.118[.]67	AS22612	Namecheap, Inc.
162.255.118[.]68	AS22612	Namecheap, Inc.
179.43.183[.]46	AS51852	Private Layer, Inc.
185.224.81[.]168	AS204196	AbleoHost B.V.
185.224.81[.]75	AS204196	AbleoHost B.V.
185.38.151[.]11	AS25369	Hydra Communications Ltd
79.133.41[.]61	AS44066	firstcolo GmbH

***Table 1**: IP Addresses and ASNs associated with new Doppelgänger domains (Source: Recorded Future)*

Similar to Doppelgänger's legacy brands, these newly observed German-language sites each frame key socio-economic and political topics — such as Germany's place in Europe, the state of the German economy, migration, and support to Ukraine — in ways that are highly relevant to German voters, reflecting thematic approaches seen in prior campaigns targeting elections in both France and the US. Specific examples include the Doppelgänger brand "Kriminal Radar", which is used to provoke German fear over safety and security, and in particular fear toward migrants. Meanwhile, Östlicher Wind is an East Germany-oriented publication that promotes feelings of Euroskepticism, distrust toward the US and Ukraine, "traditional" values, and promotion of right-wing political entities, such as AfD.

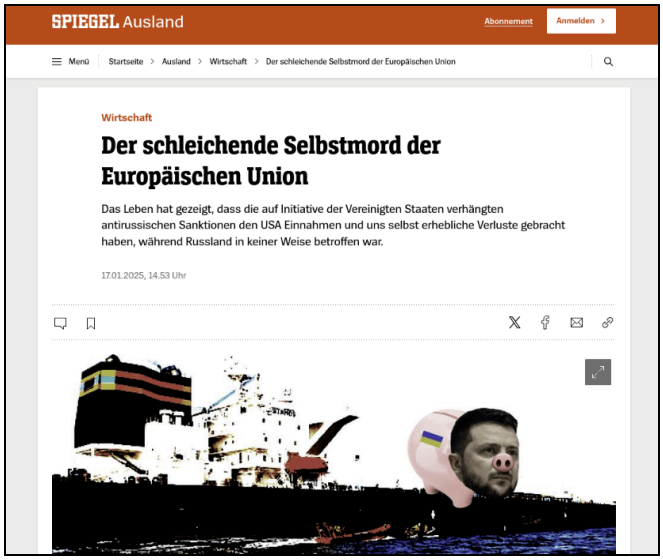
Election Issue	Doppelgänger-Aligned Branded Website	Translation
Crime, Immigration, Law Enforcement	Kriminal Radar	"Crime Radar"
Military and Security	Militärblatt	"Military Bulletin"
East/West Germany, Conservative Views	Östlicher Wind	"Easterly Wind"
German Economy	Tageswirtschaft	"Daily Economy"
German Pride	Stolzvolk	"Proud People"
Social Values	HerzHeim	"Heart Home"
World News and Germany's Global Position	WeltWahl	"World Choice"

***Table 2**: Each of Doppelgänger's new German-language "brands" thematically focuses on a core election issue for German voters (Source: Recorded Future)*

***Figures 3 and 4**: (Left) New Doppelgänger brand "Kriminal Radar". (Right) Doppelgänger brand Tageswirtschaft shares an "advertisement" for Alternative für Deutschland. Doppelgänger has incorporated external links and images posing as advertisements to make the ad seem legitimate (Source: Recorded Future)*

Impersonating Media Organizations and Leveraging Social Media

In addition to establishing new news brands, Insikt Group identified Doppelgänger activity impersonating German media outlets DER SPIEGEL and Welt via the following domains: *spiegel[.]bz*, *welt[.]cx*, *welt[.]ink*, and *welt[.]pm*. Doppelgänger's flagship influence outlet, Reliable Recent News (RRN), also continues publishing German-focused content via its website *rrn[.]com[.]tr*, on social media through the @RapidRespNews persona, and via its Telegram channel @reliablerecentnews.



***Figures 5 and 6**: (Left) Doppelgänger clone of DER SPIEGEL via spiegel[.]bz; (Right) Doppelgänger clone of Welt via welt[.]cx (Source: URLscan.io)*

Doppelgänger continues to create and operate mass social media accounts to disseminate its messages using domain obfuscation techniques Insikt Group illustrated in December 2023. Furthermore, Doppelgänger also continues to leverage various branded social media accounts that align with its Germany-oriented websites, including "Arbeitspause_1.0", "Bayerischer Löwe", and "Der Rattenfänger". Many of these personas mirror Doppelgänger's historical tactics, using localized narratives, falsified news formats, and networked amplification to increase credibility among target audiences. According to a January 2025 analysis by the German Center for Monitoring, Analysis, and Strategy (CeMAS), over 630 Doppelgänger-attributed social media posts occurred between December 2024 and January 2025, engaging in coordinated inauthentic behavior (CIB) and promoting non-credible narratives on German politics, economics, and immigration.

Operation Overload Incorporates New Tactics to Push Non-Credible Stories

From December 2024 through January 2025, Insikt Group detected dozens of inauthentic videos impersonating German and European news agencies and law enforcement, which we attribute to Operation Overload (a Russia-aligned influence operation also known as Matryoshka and Storm-1679), corroborating findings from independent researchers "antibot4navalny" and "UsHadrons", as well as from the BBC and CheckFirst. Operation Overload's social media assets are very likely actively distributing these impersonation videos to influence German public opinion and voter turnout ahead of the upcoming German federal elections. These efforts build on previous Operation Overload activities, incorporating notable evolutions in tactics, techniques, and procedures (TTPs) — including the adoption of AI-enabled voice cloning to produce audio deepfakes and an expansion beyond mainstream social media to Bluesky. Though less common than its media and law enforcement impersonation videos, Operation Overload also continues to digitally alter the front pages of European newspapers and tabloids, fabricating inauthentic leading headlines that are then disseminated on social media.

Operation Overload very likely continues to pursue two primary objectives, as Insikt Group documented in November 2024:

- Overwhelming the resources of media organizations, researchers, and counter-malign influence groups with non-credible news stories
- Influencing public opinion, either directly or indirectly, through media coverage of these non-credible narratives

Since the November 12, 2024, announcement setting the German election date, Operation Overload has very likely concentrated its inauthentic content across three primary themes:

- Concerns over the safety and integrity of the voting process
- Denigration of German coalition political parties and government leadership
- Provoking antisemitic and extremist sentiment in Germany

Similar to Doppelgänger, Operation Overload very likely considers engagement metrics — such as viewership, interactions, and media attention — to be key indicators of success. However, Operation Overload's inauthentic social media accounts lack a sustained audience, making them dependent on artificial engagement from bot networks to boost account visibility. These accounts frequently tag, mention, or direct message research communities and media organizations, requesting verification of inauthentic content as a means of garnering attention and expanding their digital reach. Additionally, coordinated networks of inauthentic accounts distribute videos as compilations of news pieces from target countries like Germany. We also assess that Operation Overload handlers likely continue to directly email researchers and media organizations, as CheckFirst documented during the operation's initial discovery.

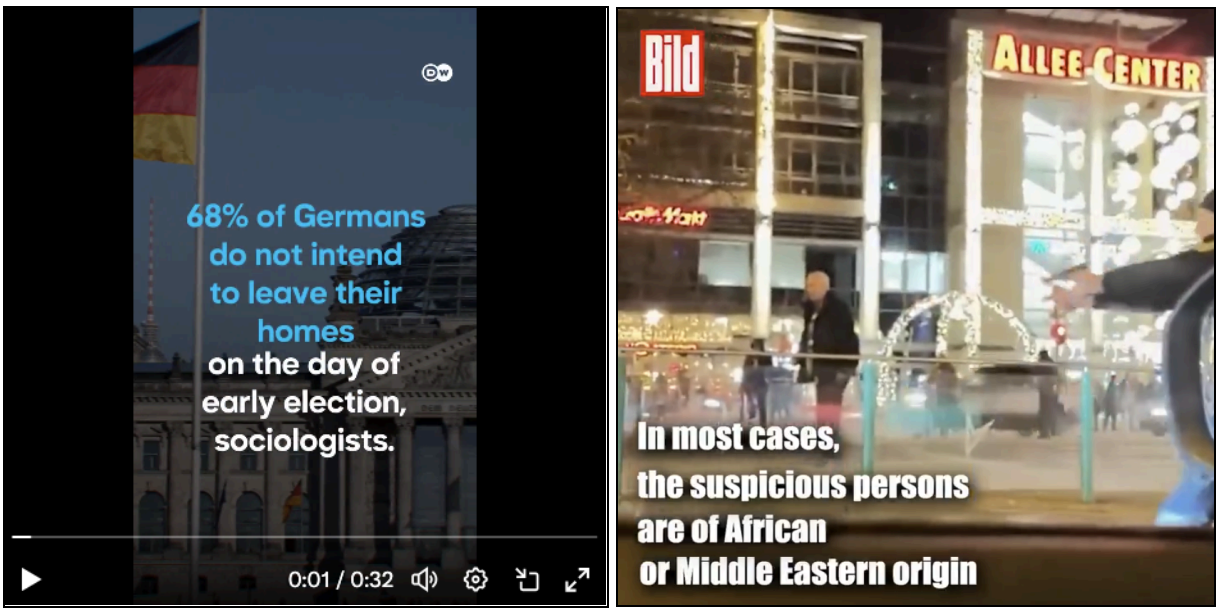
Amplifying Security Concerns and Questions of Election Integrity

Operation Overload very likely prioritizes the creation of inauthentic content that amplifies security concerns, seeking to reduce voter confidence ahead of the election. A recurring theme involves suggesting an increased risk of terrorism or other disruptive public safety incidents surrounding Election Day.

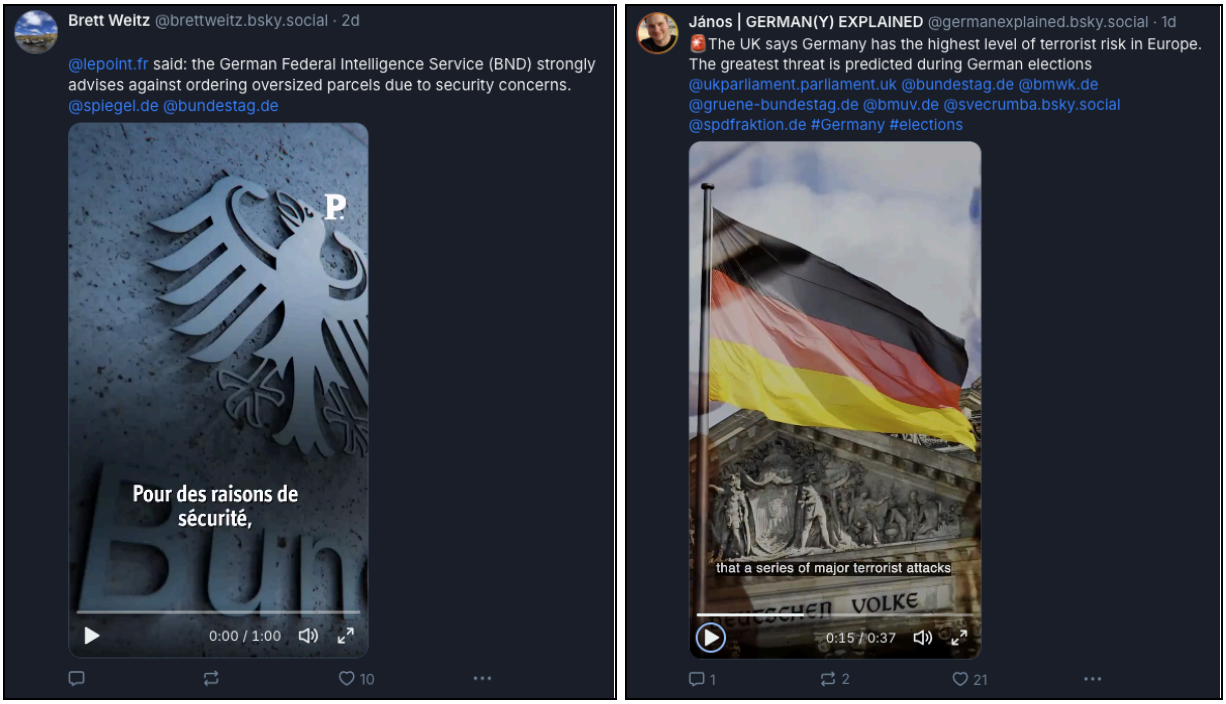
Videos reviewed by Insikt Group frequently:

- Depict German law enforcement as unprepared and overwhelmed by security threats
- Promote distrust toward immigrants and European immigration policy as vectors for security threats
- Explicitly encourage German citizens to abstain from voting under the pretense of ensuring their safety

Additionally, videos impersonating legitimate news outlets — such as a January 2025 Euronews impersonation (**Figure 11**) — seek to undermine election integrity by alleging attempted voter fraud activities. Many of these inauthentic videos closely resemble content produced ahead of the 2024 US election, which aimed to increase public safety fears and erode trust in election processes.



***Figures 7 and 8**: Operation Overload videos impersonating major German publications DW and Bild with content aligned with voter suppression techniques and distrust toward immigrants (Source: Mainstream social media platform)*

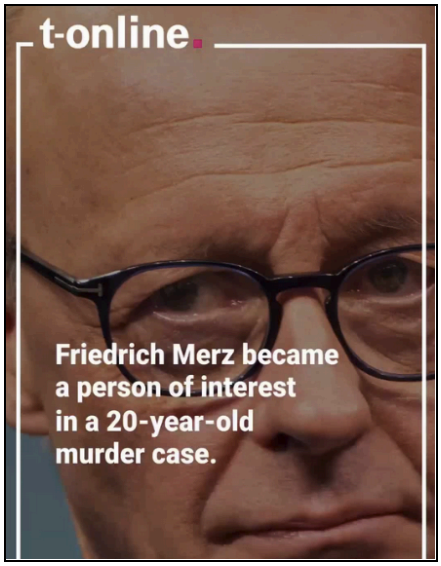


***Figures 9 and 10**: (Left) Operation Overload video impersonating French media outlet Le Point. (Right) Operation Overload video impersonating United Kingdom's West Midlands Police with content attempting to heighten public safety fears ahead of the German elections (Source: Bluesky, [archive one], [archive two])*

***Figures 11 and 12**: (Left) Operation Overload videos impersonating Euronews published to Bluesky suggest a print shop used to create pro-Green ballots was uncovered in Munich. (Right) A separate video impersonating USA Today claims the Central Intelligence Agency is alerting US citizens to avoid crowded places in Berlin during the election period (Source: Bluesky, [archive one], [archive two])*

Character Attacks on German Political Figures

Another almost certainly dominant theme in Operation Overload's efforts is the targeting of German political figures and their families with non-credible accusations of criminal activity. Videos masquerading as reports from French, German, and other European media outlets allege these individuals are involved in various illegal activities such as abuse of power, corruption, tax evasion, distribution of CSAM and pedophilia, human trafficking, and murder.



***Figures 13, 14, and 15**: Example Operation Overload videos denigrating German political figures (Source: Bluesky, [archive one], [archive two], [archive three])*

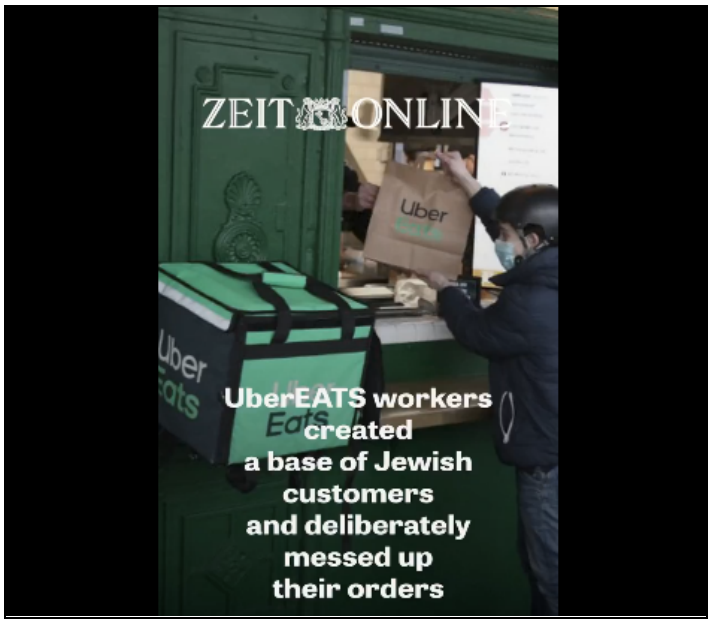
***Figures 16 and 17**: Operation Overload deceptively edited the front pages of the January 27, 2025, editions of UK tabloids Daily Record and The Sun with headlines accusing German politicians of pedophilia (Source: Bluesky, [archive])*

Manufacturing a Narrative of Rising Antisemitism in Germany and Trolling Researchers with Coded Messages

Separately, Operation Overload has promoted inauthentic content designed to portray a rise in antisemitism in Germany — this content is likely intended for international audiences. Examples include:

- Fake Bild video claiming German youth are participating in a flash mob called "I'm Not Ashamed" (#nichtpeinlich), posing with photos of Nazi grandparents
- Non-credible reports alleging Uber Eats workers in Germany have compiled a "database" of Jewish customers and are deliberately sabotaging their orders

Consistent with Operation Overload TTPs, these videos were accompanied by a QR code that also featured Zeit Online branding. This is a common tactic for Operation Overload that is almost certainly intended to give the videos an added sense of legitimacy. Typically, other elements of media branding are also included for the same purpose, such as logos and brand-specific typefaces. Surrounding the code is a string of Morse code text that, when translated from Russian, reads as a homophobic slur directed toward members of the US intelligence community. Similar findings were documented during the 2024 US elections as further evidence of Operation Overload's deceptive attempts to troll researchers.



***Figures 18 and 19**: Operation Overload videos incorporating themes of Nazi sympathizers and anti-semitism (Source: Mainstream social media platform)*

Operation Overload will almost certainly persist in producing videos impersonating German media organizations, European law enforcement, and members of the academic and counter-foreign malign influence community. However, these efforts are very unlikely to alter election outcomes, as the operation consistently fails to generate meaningful public engagement, and media and researchers

remain diligent in not treating Operation Overload content as potentially credible sources of information. That said, the potential for a significant breakout of Operation Overload content does exist, as evidenced in the recent viral spread of a video we attribute to Operation Overload that negatively depicted USAID in social media and garnered millions of views and tens of thousands of other engagements. Highlighting the operation's intended objectives and evolving tactics, does, however, remain critical to understanding and countering its malign influence efforts without overstating its actual impact on turnout or election results.

CopyCop Builds New Infrastructure to Dispense Inauthentic Content

Insikt Group detected at least 94 new inauthentic websites impersonating German-language news websites, which we attribute to CopyCop (aka Storm-1516), corroborating findings from NewsGuard, Correctiv, and Gnida Project. Following the network's focus on attempting to interfere in the 2024 French and US elections, Insikt Group assesses that the Russia-linked influence network is very likely establishing infrastructure with an intent to influence the upcoming German federal elections. Importantly, the network is likely supported by the Centre for Geopolitical Expertise (CGE) and the Main Directorate of the General Staff of the Armed Forces (GRU). CopyCop's German websites are strongly focused on covering the German election, including boosting news coverage of AfD and AfD chairwoman Alice Weidel, in addition to stoking polarizing issues such as immigration, energy policy, Ukraine, and NATO.

CopyCop Creates New German-Language Network

Insikt Group observed a significant increase in domain registrations in late 2024 with characteristics similar to known domains attributed to CopyCop. CopyCop operators began building its new German-language network on November 21, 2024, only nine days after the announcement of the snap elections, denoting the network's increased agility in responding to major political events. Between November 21, 2024, and January 5, 2025, 94 domains were registered, with fifteen domains registered on December 14, 2024, alone. CopyCop's German websites are primarily hosted on Namecheap, Hostinger, and German IT provider SIM-Networks. We observed CopyCop's German websites remain dormant or largely inactive until January 7, 2025, when the network published an initial wave of 443 posts across 74 websites.

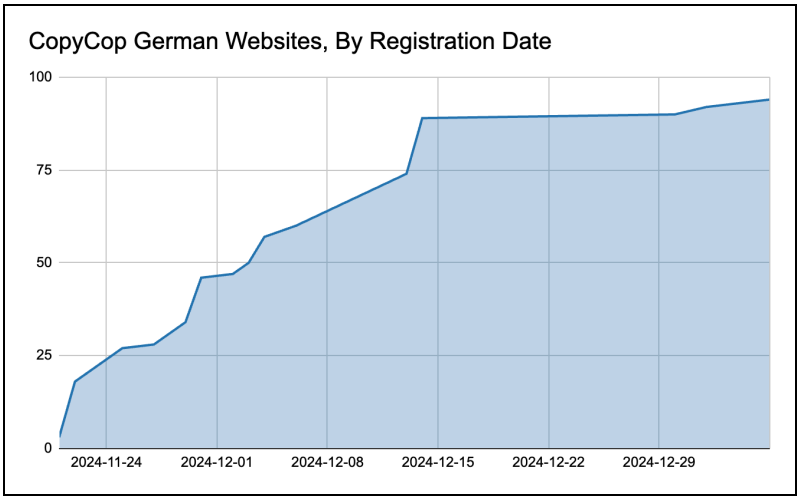
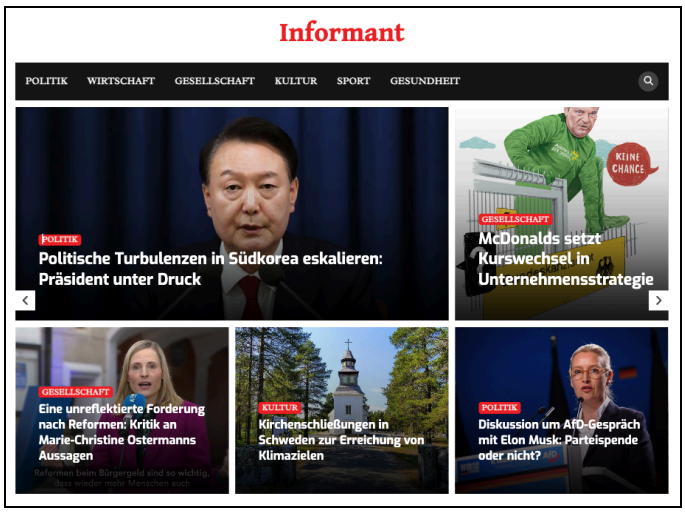
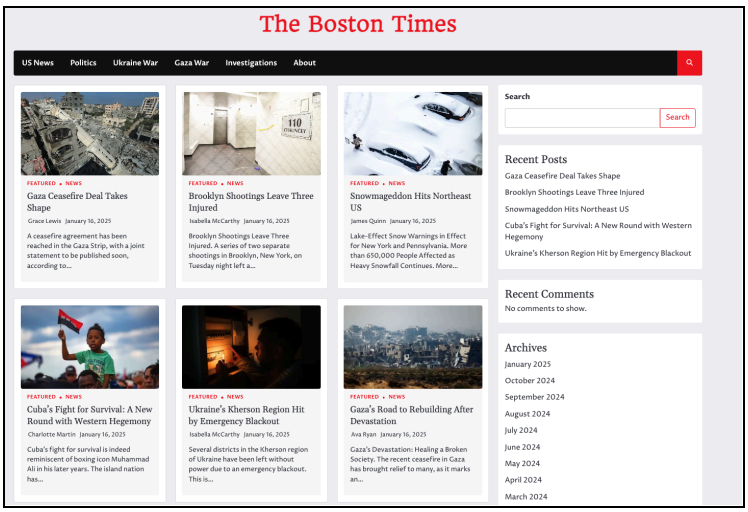


***Figure 20**: Cumulative sum of registered CopyCop German websites (Source: Recorded Future)*

Like previous CopyCop websites masquerading as local US news outlets, the 94 websites present themselves as national news outlets and media from major German cities, including Berlin, Hamburg, and Munich (see **Appendix A**). The websites are likely publishing fake media articles created using generative AI, which are then published on a scheduled basis. We continue observing evidence of large language models (LLMs) being used to plagiarize websites, including Markup syntax mistakenly used in article headers and bodies (1, 2). These fake media articles are likely plagiarized from legitimate German-language media outlets (such as Der Spiegel), AfD-affiliated outlet Deutschland Kurier and self-described Marxist outlet Junge Welt, and "alternative" outlets (such as NachDenkSeiten).





***Figures 21 and 22**: Comparison of new CopyCop website informant-info[.]de and previously attributed CopyCop website bostontimes[.]org (Source: Recorded Future, [archive one], [archive two])*

Inauthentic Videos and Deepfakes Likely to Persist

CopyCop's automated content production and scheduling pipeline enables its inauthentic websites to establish credibility with social media users. This infrastructure can also be used to amplify targeted,

human-crafted content. Examples of CopyCop content include both translated content from the Russia-based Foundation to Battle Injustice (FBR) and inauthentic videos or deepfakes depicting anonymous whistleblowers making non-credible claims about political targets. CopyCop has previously used these tactics to target German Minister of Foreign Affairs Annalena Baerbock (using *zeitgeschenen[.]de*) and to blame Ukrainians for a fictional attack on a Berlin mosque employing associated inauthentic websites (such as *berliner-wochenzeitung[.]de*).

On January 30, 2025, one of the new German-language CopyCop websites (*nrtv[.]online*) uploaded a video accusing German Vice Chancellor Robert Habeck and Bundestag member Claudia Roth of a corruption scandal involving the alleged theft of 50 valuable paintings held in storage at Berlin's Gemäldegalerie. The article suggested that Habeck and Roth assisted in facilitating the theft on behalf of Ukrainian nationals who then sold the stolen paintings to private collectors. NRTV then claimed that the gallery later received 50,000 euros (a fraction of the art's alleged value) as compensation through a bank account ultimately traced back to the Ukrainian National Bank and the United24 fund.

Insikt Group assesses that, if CopyCop follows the same tactics we observed during the 2024 US and French elections, the network will likely continue to upload deepfakes and inauthentic videos targeting German political leaders, almost certainly intensifying its efforts to circulate influence content in the days before the German elections. Dissemination methods in the 2024 elections included amplification on social media networks via major pro-Russia influencers with existing audiences like Simeon Boikov, Chay Bowes, and Tara Reade. CopyCop operators have also used additional tactics to obfuscate the origin of inauthentic videos, including paying other social media influencers to disseminate CopyCop content and likely sponsoring content on legitimate African and Middle Eastern media outlets like *elaosboa[.]com*, *almasryalyoum[.]com*, and *actucameroun[.]com*.

Operation Undercut Continues Publishing German Content

In November 2024, Insikt Group detailed a network of inauthentic accounts it tracks as "Operation Undercut", which is attributed to the SDA as an operation related to (but distinct from) Doppelgänger. Our initial report on the network identified one of the network's likely objectives as spreading content seeking to aggravate internal EU tensions, including supporting Euroskeptic political parties such as Germany's AfD and France's Rassemblement National.

Pushing Pro-AfD Content

Insikt Group has observed a continued focus on German politics by Operation Undercut accounts since the publication of our first report, although principally via the lens of German foreign policy and the war in Ukraine, which almost certainly remain the network's top priority. Content posted by Operation Undercut accounts since September 2024 on 9gag — a Hong Kong-based social media platform popular in Germany — has included headlines explicitly supporting the AfD and undermining Chancellor Scholz.

***Figure 23**: 9gag post by an Operation Undercut account attempting to undermine Chancellor Scholz in the upcoming German federal elections (Source: 9gag)*

Operation Undercut accounts also continue posting content impersonating legitimate media outlets, such as Reuters and Voice of America (**Figure 24**), to legitimize inauthentic videos discussing German politics and expressing support for AfD.

***Figure 24**: Operation Undercut video promoting AfD (Source: Recorded Future)*

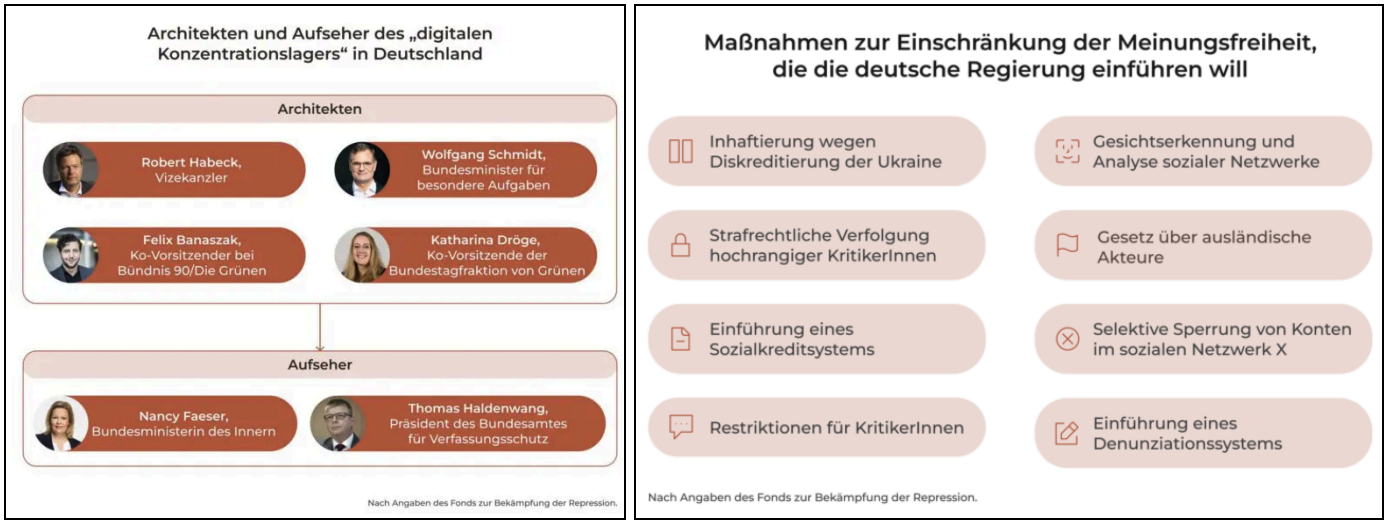
Foundation to Battle Injustice Publishes Inauthentic Investigations

The Russia-based FBR, a self-proclaimed "human rights" organization initially financed by the late Yevgeny Prigozhin and now operated by convicted money launderer Mira Terada, regularly publishes multiple non-credible "investigative" articles targeting German political parties and key figures. These reports, often citing anonymous sources, very likely aim to erode public support for certain German political leaders by undermining their reputations.

FBR's content ultimately favors political figures more aligned with Russian interests. For example, one article dated August 31, 2024, alleged that coalition party members were devising plans for "mass persecution" and assassinations of political dissidents, namely supporters of AfD.[1] [2] A separate article published on November 24, 2024, suggested that members of the ruling political coalition are planning to establish a "digital concentration camp" used to "deprive Germans of the right to freedom of speech", purportedly out of fear of a "total [election] defeat".[3] A third FBR article published on December 21, 2024, suggests that The Greens party and the political coalition CDU/CSU (the "Union parties") are planning political initiatives to "normalize" sexual abuse of minors and to lower the age of consent in Germany.

***Figure 25**: FBR article titled "The German Government Coalition Plans Legislative Measures to Normalize Pedophilia and the Abuse of Minors" (Source: Foundation to Battle Injustice[4])*

[1] *https://fondfbr[.]ru/de/artikel/germany-ampel-against-opposition-de/*
[2] *https://fondfbr[.]ru/de/artikel/german-child-abuse-de/*
[3] *https://fondfbr[.]ru/de/artikel/germany-censorship-de/*
[4] *https://fondfbr[.]ru/de/artikel/german-child-abuse-de/*



***Figures 26 and 27**: (Left) FBR article highlighting prominent German political figures as “architects and overseers of Germany’s ‘digital concentration camp’”; (Right) the same article, highlighting non-credible German government plans to restrict freedom of speech around the election period (Source: Foundation to Battle Injustice[5])*

Cross-posting for Social Media Amplification

Ahead of the 2024 US elections and into the German federal election season, Insikt Group identified articles originally published to FBR’s website cross-posted to fringe news websites, consistent with information laundering techniques, which are then used as the basis for additional amplification onto social media. The likely goal of this activity is to garner broader mainstream acceptance of FBR’s claims as “true”. The above-mentioned article alleging the ruling coalition has plans for punishing and eliminating right-wing dissidents was, as an example, supplementarily cross-posted to OKV e.V., a website featuring the logo of the Volkskammer under the former German Democratic Republic (GDR), with minimal edits to the title. The OKV e.V version was then used for additional promotion on German Telegram and Facebook pages, with later cross-posting to Pravda DE, a pro-Kremlin news portal linked to the Russian influence network tracked as “Portal Kombat”.

[5] *https://fondfbr[.]ru/de/artikel/germany-censorship-de/*

***Figures 28 and 29**: Mirror copies of the FBR article featured in **Figure 26** cross-posted to OKV e.V (top) and Pravda DE (bottom) with only slight title edits (Source: OKV e.V., [archive], Pravda DE [archive])*

Mitigations

- Media entities, the public sector, and researchers should continue to monitor content from identified influence operations and responsibly inform the public of the tactics and intentions of foreign malign influence operations.
- Some operations, such as Doppelgänger, Operation Overload, and Operation Undercut, are very likely financially bound and dependent on engagement as one metric used to justify their government contracts. Therefore, individuals of the public are advised not to engage with these networks. Bluesky labels, such as the “Matryoshka Disinfo” label managed by the counter-influence collective Antibot4navalny and validated by Insikt Group, can assist in minimizing these networks’ engagement and reach when users subscribe to the labels.
- Impersonated entities, particularly media organizations, should engage takedown services to remove or seize domains impersonating their brands.
- Impersonated entities should also engage with social media trust and safety teams to ensure targeted influence operations infringing on their branding and likeness are removed from the respective platforms.

- Media organizations can use the Recorded Future Intelligence Cloud and Recorded Future Brand Intelligence to identify potential impersonation attempts, including typosquats, logotype detection, and other potential forms of brand abuse.
- Customers can use the Recorded Future Intelligence Cloud to track each of the detected influence operations disclosed in this report and Recorded Future AI to summarize and track emerging narratives.

Outlook

As Germany's February 2025 federal elections approach, Russia-linked influence operations will almost certainly persist in their efforts to manipulate public discourse, disrupt democratic processes, and advance Kremlin-aligned geopolitical objectives. However, despite the continued evolution of tactics — such as AI-generated content, deepfake voice cloning, re-branding, and platform migration — engagement with these campaigns remains low. Their ability to meaningfully shift voter sentiment or alter election outcomes is currently very likely limited.

It is very likely that these influence networks will adapt in response to countermeasures, testing new amplification techniques, alternative platforms, and emergent AI-driven influence tools. While persistent tracking and exposure efforts by governments, researchers, and media organizations have been effective in mitigating their impact, these campaigns remain an enduring threat to the broader European information environment that will require continued monitoring, early detection, and collaborative defense initiatives. As Europe will hold several key elections in 2025, including in the Czech Republic, Italy, Romania, and Poland, continued monitoring, mitigation, and responsible disclosure to the public remain critical.

Appendix A: CopyCop Websites

```
aktuell-nachricht[.]de
aktuellde[.]de
aktuellenews-berlin[.]de
aktuelles-aus-nurnberg[.]de
alles-klar-hamburg[.]de
alles-wichtig-news[.]de
allethemen24[.]de
an-berlin[.]de
ausdemueberall[.]de
b-blatt[.]de
berlin-apropos[.]de
berlinertagespost[.]de
brlnr-stimme[.]de
cito-novit[.]de
das-denkt-hamburg[.]de
dasneueste-online[.]de
de-nachrichtenseite[.]de
deinequellen[.]de
deutsch-w[.]de
deutschenachrichtenstelle[.]de
diewahreseite[.]de
doch-infomedia[.]de
dznachrichten[.]de
einfachandersinfo[.]de
einmaleinsneu[.]de
expert-infomedien[.]de
f-aktuell[.]de
fr-press[.]de
gegengewicht-media[.]de
gegenleitmedien[.]de
guckmalgenauhin[.]de
h-np[.]de
hamb-post[.]de
hamburg-ex[.]de
hamburger-anzeiger[.]de
hamburger-sichtweisen[.]de
herrpostillon[.]de
heute-inberlin[.]de
in-absicht[.]de
in-und-ausland[.]de
info-mediaplattform[.]de
info-stichpunkt[.]de
infomediafuerdich[.]de
infomediaregierungskritisch[.]de
informant-info[.]de
```

```
ins-gesicht[.]de
internetpoebler-info[.]de
kernpunkt-infomedia[.]de
kernrecht[.]de
klartext-news[.]de
konusnews[.]de
kurzchronik[.]de
la-cher[.]de
laut-medien[.]de
media-transparent[.]de
mehrstimmen[.]de
munchener-nachrichten[.]de
n-a-h[.]de
nachrichtendestages[.]de
nachrichtenunabhaengig[.]de
news-checker[.]de
newsfuereuch[.]de
newsletters-berlin[.]de
newswichtig[.]de
nnberlin[.]de
novanachrichten[.]de
nrtv[.]online
nudis-verbis[.]de
oku-nachrichten[.]de
onlinedaheim-24[.]de
onlineunterwegs[.]de
polemisch-infomedia[.]de
presseneu[.]de
prinzipienfest[.]de
resonieren[.]de
ruf-der-freiheit[.]de
rundumdieuhr-24[.]de
sag-das[.]de
scheinwerfen[.]de
seite-eins-nachrichten[.]de
stimmedeutsch[.]de
tageblatt-berlin[.]de
tagesnews-24[.]de
tagundnacht24[.]de
thesis-info[.]de
top-news-munchen[.]de
ungeziert-info[.]de
unmittelbar-medien[.]de
vollverstand[.]de
w-a-munchen[.]de
wdr-hall[.]de
weitwinkelmedien[.]de
```

```
xn--wochenberblick-berlin-eic[.]de
zeitenwende-news[.]de
```

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 customers, 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 customers 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