FIMI RESPONSE TEAM REPORT

# Country Report: Assessment of Foreign Information Manipulation and Interference (FIMI) in the 2025 German Federal Election

FIMI RESPONSE TEAM REPORT

# FOREIGN INFORMATION MANIPULATION AND INTERFERENCE (FIMI) - INFORMATION SHARING AND ANALYSIS CENTRE (ISAC)







***Amman | Berlin | London | Paris | Washington DC***



*www.isdglobal.org*

# Authors & Partner Organizations

ISD, Alliance4Europe, Debunk.org, GMF Alliance for Securing Democracy, DEN Institute, EU DisinfoLab.

# About the Project

FDEI FIMI DEFENDERS FOR ELECTION INTEGRITY PROJECT

This country election report was developed through the project FIMI Defenders for Election Integrity. The project consortium brings together the expertise from 10 organisations to develop a multistakeholder foreign information manipulation and interference (FIMI) framework to effectively monitor, respond to and counter FIMI threats before and during elections, while simultaneously strengthening FIMI defender communities and democratic institutions. This monitoring and response also involved engaging and coordinating with 16 in-country partners from across German civil society and academia.

Over the course of these monitoring efforts, the consortium produced a series of incident alerts to be circulated to relevant election stakeholders in real-time. These incident alerts detail key information about FIMI incidents and their impact in the country of focus and provide a set of recommendations for response. Where insights derived from these incident alerts are mentioned throughout this report, they are signposted with an alphanumeric code beginning with 'IA'.[1]

# About the FIMI-ISAC

FIMI -ISAC

The FIMI-ISAC (Foreign Information Manipulation and Interference Information Sharing and Analysis Center) is the first ISAC worldwide dedicated to fighting FIMI and creating common standards in this field. It unites a group of like-minded organisations that protect

[1] While these incident alerts are not publicly accessible, the authors are able to make the findings available upon request.

democratic societies, institutions, and the critical information infrastructures of democracy from external manipulation and harm. Through collaboration, the FIMI-ISAC enables its members to detect, analyse, and counter FIMI more rapidly and effectively while upholding the fundamental value of freedom of expression. The FIMI-ISAC does not act independently to counter FIMI. Instead, enhancing collaboration empowers its members to do so more effectively.

*https://fimi-isac.org/*

**Infrastructure:**

This report and project were facilitated through the *Counter Disinformation Network*. The CDN is a collaboration and crisis response platform, knowledge valorisation resource, and expert network, bringing together 58 organisations and over 300 practitioners from OSINT, journalism, fact-checking and academia from 25 countries. The network has been used to coordinate projects on four elections and has produced 76 alerts since its creation in May 2024.

# Table of Contents

# Executive Summary

The 2025 German federal election took place in a volatile political landscape marked by multiple geopolitical crises, economic uncertainty and declining trust in institutions. This report by ISD and contributing organisations offers a comprehensive analysis of the foreign information manipulation and interference (FIMI) that shaped the pre-election period. It examines the motivations behind these influence operations, the actors involved, the techniques employed and the broader impact on democratic discourse and electoral integrity.

Foreign and domestic actors exploited existing societal divisions—particularly around migration, economic instability and national identity—by deploying coordinated campaigns and leveraging digital platforms to spread disinformation. Key operations such as Operation Overload, Storm-1516 and Doppelgänger were instrumental in disseminating misleading narratives and manipulating public opinion. They often made use of tactics such as AI-generated content, impersonation of credible institutions and abuse of social media infrastructure.

Themes in disinformation narratives included electoral fraud, anti-migrant sentiment, economic collapse, support for Ukraine and the delegitimisation of democratic institutions. We found it particularly concerning that campaigns integrated AI-generated content and bot networks and that sanctioned outlets such as RT DE (formerly RT Deutsch) continued to reach German audiences and diaspora communities in Germany despite being officially banned.

Given the often significant interaction between FIMI actors and domestic communities, the report highlights tactics employed by foreign entities as well as the selective and strategic adoption of similar approaches by domestic actors, including the right-wing populist Alternative für Deutschland (AfD) party. Despite efforts from civil society, regulators and platforms, significant gaps in policy enforcement and platform accountability remained.

To safeguard democratic integrity, the report recommends a coordinated, multi-stakeholder approach involving regulatory reform, enhanced transparency, media literacy and long-term investment in democratic resilience.

# Key findings

- **High-impact narratives:** Migration, national security, Ukraine and economic collapse were among the most manipulated themes, with the apparent aim of the electorate and undermining democratic legitimacy.
- **AI and media manipulation:** Deepfakes, AI-generated video and audio and impersonation of media and academic institutions were used to fabricate credible-seeming content.
- **Coordinated FIMI operations:** Campaigns from Russia-aligned actors (Operation Overload, Storm-1516 and Doppelgänger) exploited social media to spread disinformation. This often included bot networks and influencer amplification.
- **State media influence:** Despite EU sanctions, RT DE maintained influence through mirror sites and alternative podcast networks, highlighting enforcement gaps.
- **Political actor misconduct:** The AfD employed AI-generated content and impersonation strategies similar to foreign influence operations. This blurred the lines between legitimate and deceptive campaigning.
- **Inflated metrics and inauthentic engagement:** Engagement figures were often artificially boosted, distorting the perceived reach and legitimacy of disinformation content.
- **Limited platform enforcement:** With fairly limited data, this report assesses that mainstream platforms failed to act on flagged content. Emerging platforms such as Bluesky showed more proactive responses.
- **Policy gaps identified:** Weak enforcement of sanctions, underresourced regulators and limited transparency in digital political advertising hindered effective responses.
- **Whole-of-society approach required:** **Long**-term funding, cross-sector cooperation and institutionalised resilience strategies are essential to countering future influence operations.

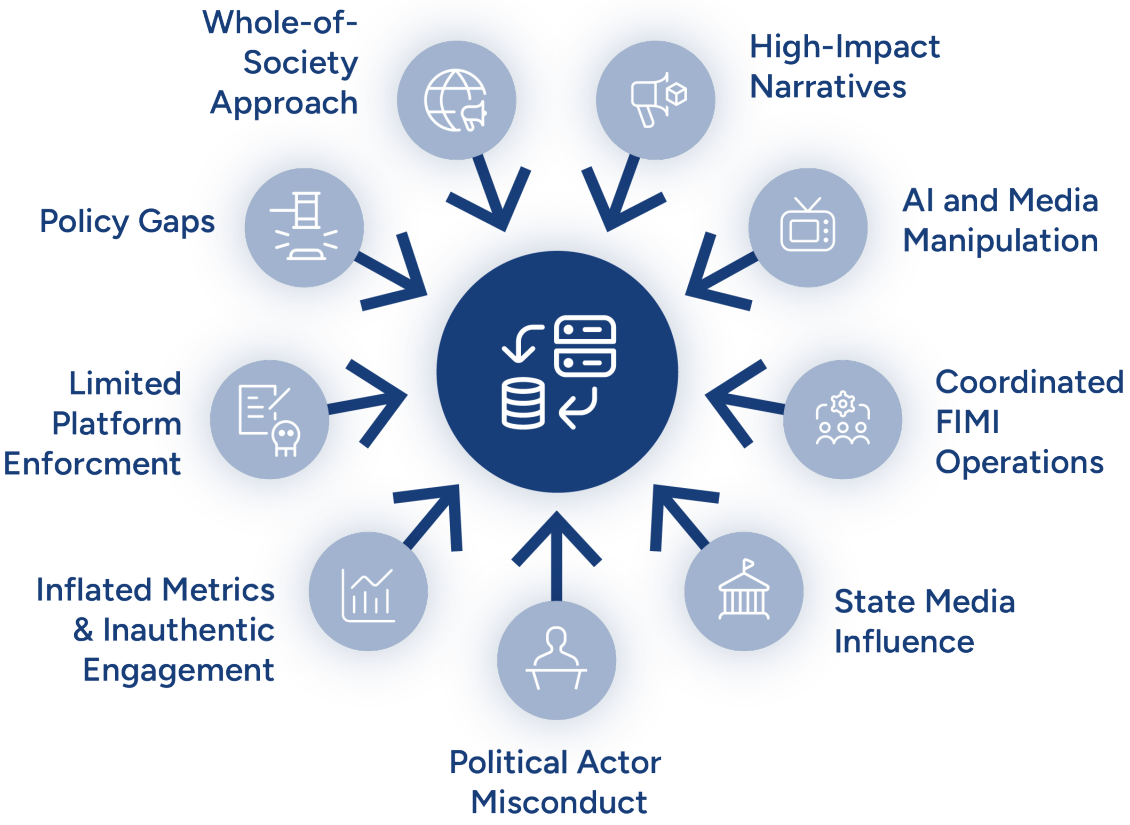



*Figure 1: Poland's Strategic Geopolitical Exposure*

# Introduction

Germany continues to face ongoing challenges related to safeguarding information integrity. As noted prior to the federal election in February 2025, the country faces factors including economic uncertainty, the ongoing war in Ukraine, increasing geopolitical tensions and debates over immigration policy. These have fuelled public discontent, shaped political discourse and provided ground for the spread of disinformation, further deepening societal divisions.

This report assesses the key risks that emerged from FIMI in relation to the 2025 German federal election. It examines the incentives and mechanisms behind influence campaigns and the role of digital platforms in spreading misleading narratives. It highlights prevalent disinformation narratives, such as those related to migration, national security, economic instability and democratic legitimacy. The report then provides further analysis of the techniques used to amplify these narratives including AI-generated content, social media manipulation and selective framing. It outlines observed coordinated operations active during the election period (including Operation Overload, Storm-1516 and Doppelgänger) shedding light on their structure and impact. The report also discusses sanctioned Russian media outlet RT DE's at least partially successful attempts to circumvent sanctions to make content available to German audiences and diaspora communities.

Furthermore, the report provides insights into instances of unfair conduct by political actors and assesses the broader impact of disinformation campaigns. It also reviews interventions and responses implemented during the election period, including those documented in incident alerts.

Finally, the report concludes with policy recommendations aimed at regulators. In doing so, it provides a comprehensive assessment of Germany's evolving political landscape. It outlines the necessary steps that law enforcement, platforms and civil society should take to safeguard democratic integrity and public trust.

To provide data-driven context and analysis for the 2025 election, 100 public reports on FIMI from the 2017, 2021 and 2025 federal election were collected, codified and processed by threat intelligence platform OpenCTI to identify new and persisting trends. These public reports were made up of 80 media reports and 20 real-time incident reports generated in the 2025 election. Based on these reports, 98 specific incidents of foreign information manipulation and interference (FIMI) were identified. This exercise also identified 198 STIX Domain Objectives – threat actors, malware, attack patterns (TTPs), incidents, indicators, campaigns, tools and vulnerabilities – and 2,554 relationships between threat actors, attack patterns and narratives in the reports.

# Incentives and enablers of FIMI

## Geopolitics and domestic vulnerabilities

Entering the election period, Germany was affected by widespread *political discontent*, *economic concerns* and societal divisions. All of this created fertile ground for information manipulation by foreign actors seeking to destabilise democratic processes and institutions.

Previous research has shown that older adults and those with distrust in media are particularly vulnerable to disinformation: they struggle to distinguish credible from false information, rely on unverified digital sources and are more likely to engage with manipulative narratives and alternative information ecosystems. A 2025 study shows that young people and users of TikTok are vulnerable to pro-Russian and pro-Chinese disinformation as well as conspiracy narratives.

This lack of institutional trust creates fertile ground for alternative narratives and extreme worldviews that question Germany's existing democratic system at its core. Such distrust also heightens the risk of FIMI: external actors exploit public disillusionment to amplify polarisation, spread disinformation and undermine confidence in democratic institutions. For example, posts made as part of the Russia-aligned Operation Overload aimed at undermining trust in public safety during the *2025 Federal Elections.* Other FIMI campaigns claimed election fraud by specific parties: a video and article published on 21 February 2025 by the Russian state-aligned Foundation to Battle Injustice (R-FBI) claimed that the Green party was planning to commit electoral fraud. Foreign actors might undertake such actions to gain a geopolitical advantage through weakening the social cohesion of nations they see as adversaries.

There is a perception of higher vulnerability to false and misleading content in some German states, particularly in Eastern Germany. This is influenced by historical and socio-political factors such as greater institutional distrust and historical ties with Russia. These factors contribute to a complex media landscape where alternative news sources can exploit social grievances, potentially targeting vulnerable communities with anti-migrant, anti-government and Covid-19-related misinformation.

Additional factors include the income, employment and opportunities gap between rural and urban voters and the perception (common across Western European countries) that *central governments care less about rural populations.* As a result, rural voters may be more vulnerable to the *anti-establishment narratives* commonly used by influence

operations. Some campaigns used such narratives alongside the broader political discussion around the election to spread pro-Russian and anti-Ukrainian propaganda in the context of the ongoing conflict in Ukraine. A Doppelgänger campaign observed from 28 December 2024 until 5 January 2025, encompassing 288 X posts, stoked fear of economic ruin in Germany, connecting this narrative to countries' support for Ukraine (IA0038). In some instances, *verified accounts on X (formerly Twitter) were used to spread pro-Russian narratives.* Propagating favourable viewpoints of the respective foreign actor and thus swaying public opinion in their favour is another goal of foreign influence operations.

## Political motives

A range of incentives and enablers have driven FIMI activities targeting the German federal elections. Geopolitical objectives appear central with some foreign actors aiming to destabilise Germany and by extension the European Union (EU). Campaigns often sought to portray Germany and the EU as unstable: this included narratives about *alleged terror threats* targeting Germany during the election period, alongside disinformation concerning the country's supposed economic and *political decline.*

Political motives are also evident in efforts to undermine trust in democratic institutions and strengthen fringe parties and opposition forces, particularly the AfD. Videos posted on X and Bluesky by accounts associated with Operation Overload endorsed the AfD (IA0049), while other Russia-aligned operations (including Doppelgänger) targeted and disparaged *other parties.* As discussed below, this type of information manipulation can also be motivated by financial incentives: disinformation campaigns can be monetised through increased traffic and engagement, benefiting affiliated networks.

While the amplification of divisive narratives from the AfD campaign by individuals and organisations outside of German politics is a *recurring pattern*, a key actor in this regard was Elon Musk. In the lead-up to the elections, the Atlantic Council's Digital Forensic Research Lab (DFRLab) *published a report* on the so-called 'Musk Effect', detailing how Musk used his own audience and influence on the platform X to empower the AfD and increase engagement with its leader, Alice Weidel, including by hosting a *live discussion* with Weidel two weeks prior to the vote.

## Financial incentives

The German elections were set against a backdrop of economic uncertainty, including inflation and ongoing conflicts in Ukraine and the Middle East. These factors left segments

of the electorate particularly vulnerable to information manipulation and propaganda related to economic conditions, immigration and geopolitical issues. Some influence operations specifically targeted economic anxieties. Between 9 January 2025 and 19 January 2025, the Russian Doppelgänger influence campaign shared authentic and inauthentic articles on X (IA0042). These articles discussed economic issues, with many claiming that Germany's economy was weak.

FIMI operations do more than discuss economic and financial issues; foreign actors also set financial incentives for furthering their propaganda efforts. Russia has financially supported war influencers (so-called *'ZBloggers'*) in the context of its invasion of Ukraine. In general, social media platform engineering can financially incentivise malign actors to spread mis- and disinformation, with the promise of monetisation through engagement. This includes foreign-originated content and commercial networks designed to amplify such content. Thus, actors not financed by foreign governments may still be financially motivated to conduct influence operations.

The Russian government has sought to foster *division and polarisation in Germany in recent years* and has a strong incentive to bolster pro-Kremlin political forces and *amplify divisive narratives.* Although sanctions have somewhat curtailed Russia's ability to exert overt influence in Europe, there is substantial evidence that the Kremlin has dedicated significant resources to circumventing these restrictions and establishing infrastructure for covert influence operations. In some cases, foreign actors like RT were able to circumvent sanctions through social media platforms. As Alliance4Europe found during the monitoring period for this project, RT DE created a new X account in January 2025 and used the account to promote its circumvention sites and mock the EU's sanctions on Russia (IA0039).

# Common FIMI narratives

During the monitoring of the German federal elections, several recurring disinformation narratives were identified. These narratives appeared to be strategically crafted to influence the electoral process in favour of Russian interests, therefore favouring the AfD and Bündnis Sarah Wagenknecht (BSW). However, many are common narratives that resurface time and time again in German election cycles.

The visual on the next page depicts the five most prominent narratives in content monitored by analysts during the 2025 federal German election cycle, based on a qualitative assessment.


*Figure 2: Prominent narratives in German election discourse that are commonly leveraged by foreign actors*

## Immigration

One recurring narrative centers on the issue of migration, which was featured prominently during the German election campaign in general. The debate intensified with the proposed Zustromsbegrenzungsgesetz ("Influx Limitation Act") brought by the Christian Democratic Union (CDU) and Christian Social Union (CSU) parliamentary group which aimed to tighten migration policy. Controversies escalated during the bill's second reading when it received support from the AfD. Although the bill ultimately failed, the AfD's backing sparked significant public and political backlash: it was seen as breaching the informal cordon sanitaire that traditionally prevents mainstream parties from cooperating with extreme right-wing actors.

Disinformation campaigns use the issue of migration to amplify public fears in a way which aligns with the AfD's agenda. During the lead-up to the German federal election, this narrative was picked up by several operations discussed throughout this report. *A recent analysis* on the Russia-linked Doppelgänger network, *released* by the German Federal Foreign Office, identified migration as a key focus alongside anti-Ukraine and pro-Russian narratives.

These anti-migrant narratives echo those identified in German far-right spaces: these typically vilify migrants from the Middle East and Africa, while specifically pushing pro-Russian narratives *depicting* Ukrainian refugees as a threat to the country. The same campaign, which operated a coordinated network of inauthentic accounts on X, actively sought to bolster support for the AfD by exploiting migration fears. Russian disinformation campaigns aimed to influence voter turnout and polarise the public debate by capitalising on such fears, particularly after a string of *pre-election attacks involving foreigners* in Mannheim, Munich and Aschaffenburg. These tactics mirror established disinformation strategies used in past European elections by *foreign state actors* in an effort to manipulate voter sentiment.

## Anti-government and antiestablishment

Anti-government narratives from FIMI actors typically depict a world in decline, with Western nations (particularly France, Germany the US and Ukraine) facing economic, political and military catastrophe. France has been portrayed as *collapsing under President Emmanuel Macron's leadership*, suffering economic ruin, losing influence in Africa and recklessly endangering lives in Ukraine.

The German establishment is *framed as corrupt* with narratives framing politicians as working solely for personal gain. These narratives claim that Germany has been

impoverished and economically crippled by the ruling 'traffic light' coalition, by pushing for anti-Russian sanctions and support for Ukraine. Campaigns like Operation Overload or Doppelgänger do not spare the CDU/CSU from such framing: they highlight Angela Merkel's past migration-friendly policies and the party's current aspirations as the root cause for Germany's steady financial and societal decline. At the same time, these sources frame Ukraine as corrupt, undemocratically governed, militarily doomed and *abandoned by allies.* These narratives collectively aim to undermine *Western unity*, destabilise support for Ukraine and amplify distrust in democratic institutions.

## Election integrity

False claims related to election tampering, fraud and 'rigging' have been among the most persistent narratives in election cycles in the West over the past few years and Germany is no exception. In this context, fabricated and manipulated photos, videos and audio are often used to disseminate inaccurate or decontextualised claims about election integrity. Alleged mail-in voting fraud, purportedly unsafe ballot boxes and falsified ballots or vote counts are recurring themes in disinformation. The narratives aim to undermine public trust in democratic processes and institutions.

Examples of such false information during the 2025 German elections included several *videos* which falsely claimed that the option to vote for the AfD was missing from ballots in Leipzig. Other *videos* claimed to show that ballots containing AfD votes shredded in Hamburg. These ballots were identified as inauthentic by the Bundeswahlleiterin ("German Federal Returning Officer"), as communicated by *independent fact-checking organisations* as well as two separate press releases by the cities of Leipzig and Hamburg. Investigative efforts by Correctiv and the Gnida Project *traced* these accounts to Russia's Storm-1516 campaign, *noting* their previous content shared hallmark features associated with the operation and websites attributed to it.

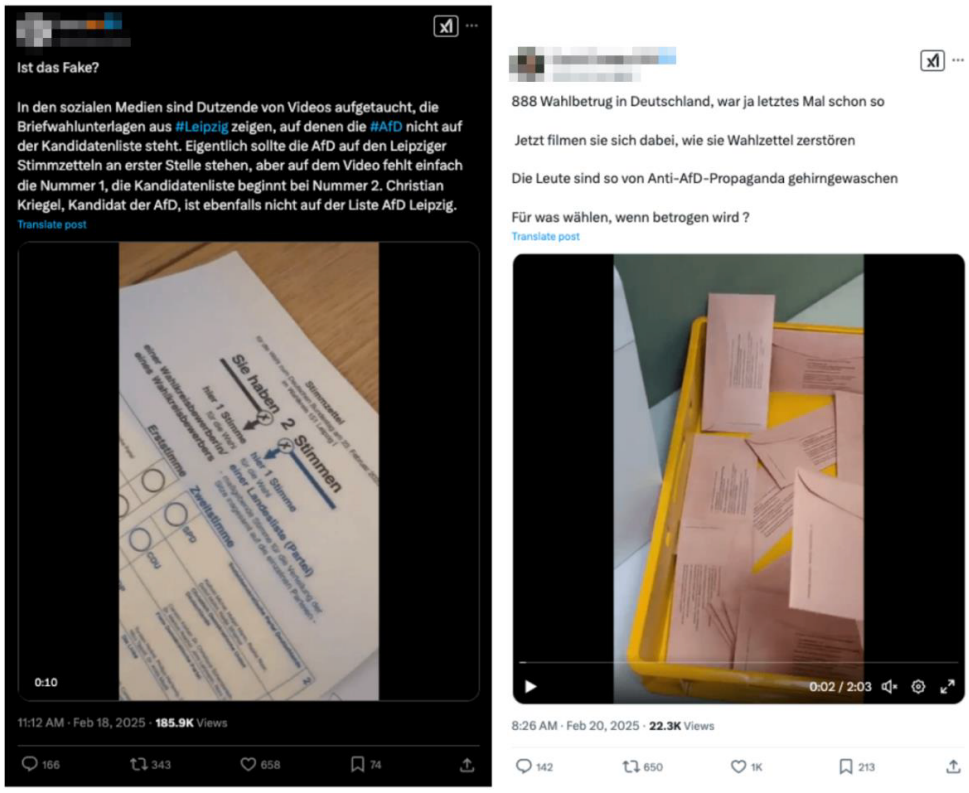
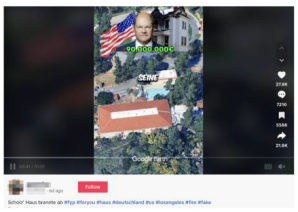



*Figure 3 (left)[2] and 4 (right)[3]. X posts claiming AfD votes were missing on Leipzig ballots or being shredded in Hamburg. Source: Correctiv.*

Disinformation campaigns frequently target political candidates as well as the electoral process itself (see table X). False statements regarding candidates' policy proposals and major campaign issues, such as migration and climate change, are commonly spread during electoral cycles, as are fabricated or misleading quotes. Candidates from the Green party have been a particular focus of such campaigns, often portrayed as out of touch or accused of pushing harmful agendas — especially in relation to environmental policy and support for Ukraine.

[2] Translation: "Is this fake? Several videos have appeared on social media showing postal voting documents from #Leipzig in which the #AfD is not on the list of candidates. The AfD should actually be at the top of the Leipzig ballot papers, but the number 1 is missing on the videos, with the list of candidates starting at number 2. Christian Kriegel, an AfD candidate, is also not on the Leipzig AfD list. "
[3] Translation: "888[th] Election fraud in Germany, just like last time. Now they're filming themselves destroying ballots. People are so brainwashed by anti-AfD propaganda. Why vote when there's fraud? "

| Politician | Party | False or misleading narrative | Example |
|---|---|---|---|
| ***Friedrich Merz*** | Christian Democratic Union of Germany (CDU) | German conservative opposition leader Friedrich Merz was hospitalised in 2017 for attempted suicide. |  [4] |
| ***Olaf Scholz*** | Social Democratic Party of Germany (SPD) | German Chancellor Olaf Scholz owned a villa in Los Angeles that burnt down during the 2025 California wildfires. |  |
| ***Marcus Faber*** | Free Democratic Party (FDP) | Marcus Faber, a member of parliament for the German Liberal Democratic Party (FDP), works as an agent for Russia. |  [5] |
| ***Frank-Walter Steinmeier*** | Social Democratic Party of Germany | German President Frank-Walter Steinmeier threatened to nullify the 2025 German federal election. |  [6] |

[4] Translation: "Friedrich Merz attempted suicide in 2017 - German psychiatrist presents new details on the CDU chairman's hospitalisation and his diagnosis of an emotionally unstable personality disorder. "
[5] Translation: "Is Defence Committee chief Faber working for Russia? Video accusations have surfaced"
[6] Translation: "Steinmeier threatens: Election could be cancelled if the WRONG party wins. Is this still democracy? This is an announcement of deliberate electoral fraud! "

| | | | |
|---|---|---|---|
| **Robert Habeck** | Green Party | Green Party Candidate Habeck sexually abused Milina Craz. | *"For example, in a false article and video, Green party candidate Robert Habeck was accused of having abused a young woman years ago."* |
| **Robert Habeck** | Green Party | The German Green Party helped Ukraine steal 100 million euros worth of paintings from a Berlin museum. | *"A German-language website, nrtv.online, published an article and video falsely claiming that the Green Party politicians Robert Habeck and Claudia Roth had been involved in a scandal over missing paintings from Berlin's Gemäldegalerie Art Museum."* |
| **Annalena Baerbock*** | Green Party | Foreign Minister Annalena Baerbock met with a gigolo during trips to Africa. | *"Other baseless claims promoted by the campaign were that foreign minister Annalena Baerbock met with a gigolo during trips to Africa"* |
| **Claudia Roth** | Green Party | The German Green Party helped Ukraine steal 100 million euros worth of paintings from a Berlin museum. | *"A German-language website, nrtv.online, published an article and video falsely claiming that the Green Party politicians Robert Habeck and Claudia Roth had been involved in a scandal over missing paintings from Berlin's Gemäldegalerie Art Museum."* |

## Gendered disinformation

The targeting of former Federal Minister for Foreign Affairs Annalena Baerbock highlights the specific targeting of female politicians by information operations. Baerbock has been a target of gender-based discrimination and disinformation throughout her career, with reports from *Alliance for Securing Democracy* and ISD in 2021 outlining *various narratives* that targeted her in that year.

As noted in these reports, a common strategy used by information manipulation actors is to single out women candidates using false, gender-based narratives about their sexuality and appearance. In the 2025 election, accounts and websites associated with Storm-1516 claimed that Baerbock met with a gigolo during her trips to Africa. This claim was *spread widely*, along with other narratives targeting Baerbock's Green Party colleagues including Robert Habeck.

Gendered disinformation can have *serious consequences* for female politicians: these narratives are not only misogynist but also *target women disproportionately* (compared to their male colleagues) to intimidate them and limit women's access to both the political and public sphere. Beyond the individual impact, such attacks can discourage other women from *participating in public life*, contributing to a broader silencing effect and reinforcing existing gender-based barriers to participation.

## Case study: defamation of key political figures

One *example* of targeted disinformation that circulated in the lead-up to the 2025 German elections was the false claim that Olaf Scholz had called on Germany's parliament to declare a state of emergency. Additionally, *false reports* circulated claiming Scholz's house in Los Angeles had burned down in the regional wildfires and that he intended to sue the US over the incident. In reality, the videos circulating actually showed the LA Police Academy. In January, a *photo* of Scholz reaching out to Baerbock was cropped and misleadingly framed to suggest that she was refusing to take a photo with him and was leaving the meeting. In reality, Baerbock was engaged in conversation with someone else when the then-chancellor attempted to get her attention.

Further videos posted by accounts linked to the Storm-1516 campaign and the R-FBI *made allegations* of abuse against the CDU's Friedrich Merz, Green Party's Robert Habeck, Die Linke politician Janine Wissler and Armin Laschet, a former CDU chancellor candidate then running for parliament.

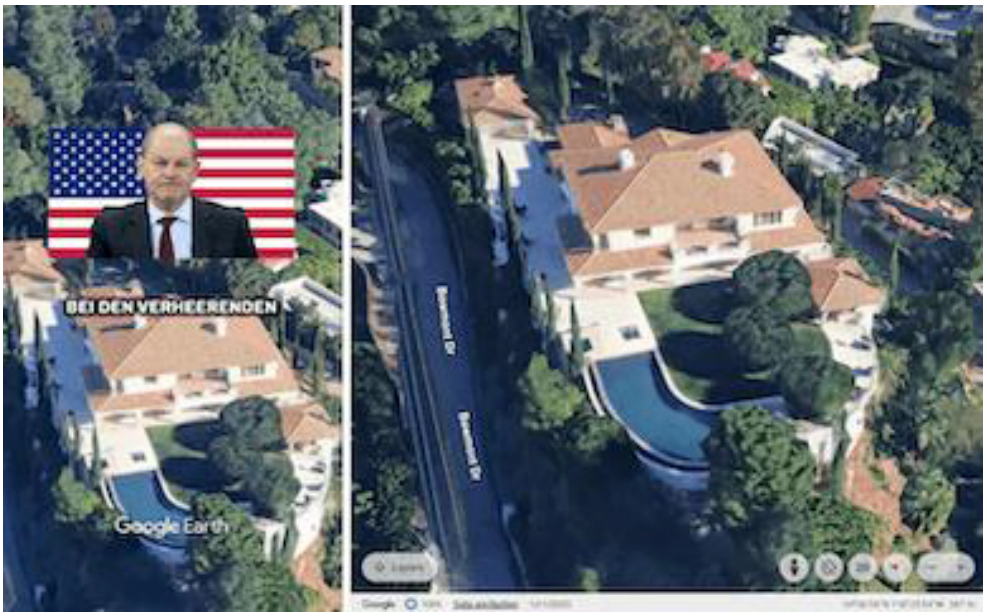



*Figure 5. Post showing Scholz's alleged mansion in Los Angeles. Source: Correctiv.*


*Figure 6: Allegations of abuse aimed at Robert Habeck (Greens).*[7]

## Geopolitical conflicts (Ukraine, Israel-Hamas)

Geopolitical conflicts, especially the ongoing war in Ukraine, were weaponised by FIMI operators to spread false information. Since the war began, Russian state-backed groups have *ramped up their efforts* to manipulate public discourse and shape the *information landscape across Europe.* Given its political influence, Germany has been a primary target especially in the lead-up to the 2025 election.

Pro-Kremlin actors were found to have continued attempts to fuel division and polarisation, aiming to weaken German support for *Ukraine*. State-backed disinformation campaigns across Western countries frequently *targeted* Ukrainian President Zelensky and his wife: false claims included that they lead a lavish lifestyle, buying *million-dollar yachts* or going on *luxury shopping sprees*, while Ukraine relies on financial support from the West.

[7] Translation: "In a harrowing video, 18-year-old Milina Adelina Graz, a pupil at a grammar school in Brunsbüttel, revealed a traumatic experience from her childhood. She talks about a sexual assault by the then Environment Minister of Schleswig-Holstein and current Economics Minister of the Federal Government Robert #Habeck, which allegedly took place during Ringelganstage in 2017. Now it's even clearer that @Die_Gruenen are a pool of paedophiles!! It remains to be seen how politicians and the Greens will react to these shocking allegations. Robert Habeck has not yet issued a statement."

Other FIMI campaign narratives focused on discrediting sanctions against Russia. These attempted to portray sanctions as ineffective against Russia and harmful to the West, depicting Ukraine as weak or already defeated while imagining Russia as superior military and a defender of traditional values. These campaigns advocated for peace negotiations with Russia, often excluding Ukraine. Support for Ukraine was framed as an economic burden on Germany and an escalation of the conflict. Pro-Ukraine German politicians, including Robert Habeck and Claudia Roth (both members of The Green Party) were accused of committing crimes against Germans to provide funds for Ukraine, with one narrative alleging that the two politicians helped Ukraine steal *100 million euros worth of paintings* from Berlin's Gemäldegalerie Art Museum. These campaigns also promoted the AfD and BSW ahead of the German federal elections, spread claims that global sympathy for Russia was increasing and that there was a rising alliance of right-wing politicians worldwide.

The conflict in Ukraine was not the only international issue that shaped the election period and the accompanying disinformation narratives. Elements of the Russia-linked Doppelgänger operation also spread disinformation aimed at presenting the Middle East as rapidly *descending into chaos* and Israel's *geopolitical position* as weakening.

## Energy and economy

The monitoring phase of this project also concluded that narratives related to economic weakness in Germany were prevalent. An *operation likely linked to Doppelgänger* on X fueled this narrative with false claims. Common arguments focused on the decline of once-strong German companies, mass job losses from indifferent banks, a weakening car industry, impending worker shortages due to retirement waves, fiscal irresponsibility across all German parties and a drop in demand for electric vehicles.

# Threat actors

Several threat actors were identified as having conducted FIMI in the context of the 2025 German federal election. These included Russia-aligned information operations, namely Doppelgänger, Operation Overload and Storm-1516. High-profile figures like Elon Musk are also likely to have played a role in amplifying support for the AfD. This underscores the increasingly blurred lines between coordinated information manipulation and elite-driven traditional influence through major social media platforms.

## Russia-aligned actors and assets

Russia was consistently identified as the top threat actor targeting German elections over the 2017, 2021 and 2025 elections, employing a variety of means throughout this period.

This project found that in 2025, Russia's approach to Germany was focused on its support for Ukraine and status as a key Western country in the EU and NATO. Many operations focused on supporting and amplifying the narratives and rhetoric used by the AfD, which draws a significant portion of its base from Eastern Germany. However, support for the extreme right-wing party increased throughout Germany with many pro-Russian narratives in its messaging. The narratives that the AfD is the only party that can run Germany effectively and that Germany's traditional political elite are corrupt were used to support Russia's goal of diminishing anti-Russian forces in the German political sphere. This approach also supported its aim of creating a pro-Russian German government with which it can resume more normal relations, including the sale of gas.

## Doppelgänger

*Doppelgänger* was not formally recognised until 2022 with the full-scale invasion of Ukraine. However, Russia-aligned operations of this type were present in Germany prior to this: German news agency Der Spiegel has been a *long-running target* for impersonation attempts originating from Russia. Doppelgänger was active in Germany prior to the 2025 federal election. However, the scale of its activity increased in the lead-up to the election in an attempt to influence voters by spreading pro-Russian narratives through media websites designed to look like trusted media platforms. A report by Recorded Future assesses that Doppelgänger leveraged *seven new inauthentic news brands* to exert influence over the German information space over the course of the election, in addition to the usual impersonation activities.

## Operation Overload

Operation Overload was also active in Germany before the 2025 federal election, but the scale of its activity increased in the few weeks prior to the vote.

Overload typically works to flood research organisations, election NGOs and media outlets with inauthentic reports of election interference and tampering. The goal is to limit their abilities to actively respond to real threats to the election. In the German context, the campaign employed *AI-powered impersonation* techniques on X: it deployed more than 50 accounts to promote claims that election officials, law enforcements and NGOs were unprepared for terror threats or election fraud or even complicit in covering them up. These posts were artificially amplified by a secondary network of around 6,000 inauthentic accounts. These inauthentic reports were primarily found in English, indicating that they were designed to skew international media narratives and preemptively discredit German democratic institutions.

## Storm-1516

Storm-1516 was also active in the federal election and is known for producing manipulated and staged videos to seed false claims about election candidates and processes. The operation has previously been identified as a threat actor in contexts including *the Paris Olympics*, the US 2024 presidential election and the *conflict in Ukraine.*

In Germany, an *investigation by Correctiv and Newsguard* uncovered that Storm-1516 had established more than 100 websites producing AI-generated content and disinformation over at least the three-month period prior to the election. The content frequently promoted the AfD and targeted Green Party candidates for their support of Ukraine and NATO. Articles on one site included claims that Green Party candidate *Robert Habeck sexually abused a woman* and that Germany planned to import *1.9 million Kenyan workers.* Accounts associated with the operation also spread a claim about a *100 million Euro corruption scandal* and attempted to implicate German politicians including Habeck and Claudia Roth.

Other Storm-1516 activity observed in the German federal elections closely imitated that seen in *the most recent US election.* Videos produced by the operation in the days before the election included claims of ballot or voter fraud in German cities such as *Hamburg and Leipzig.* These echoed previous operations targeting the US states of *Pennsylvania* and *Georgia.*

The ways in which election candidates were targeted also bear similarities. For example, the baseless allegation that German Green Party candidate Robert Habeck had sexually assaulted a woman mirrors a similar campaign launched against former US vice-presidential candidate Tim Walz, who was *falsely accused* of assaulting a student.

## High-profile amplifiers

A number of individuals and organisations based outside of Germany may have had an impact on the information environment in the weeks leading up to the election. While these high-profile amplifiers are not typically considered as FIMI actors, their influence is significant and cannot be excluded from the analysis.

The most obvious example of this was Elon Musk, who publicly *declared his support for the AfD* and hosted a live discussion with party leader Alice Weidel. While X has limited reach and influence among German voters, Musk's content gained outsized attention in traditional and online media. This helped to legitimise and spread AfD-aligned narratives beyond the platform itself. It is difficult to assess the impact of this support without greater access to platform data: however, it is likely that Musk's involvement at a time when he was both a *US government representative* and the owner of a major social media platform boosted the party's credibility in Germany and internationally.

An *anecdotal example* of this credibility boost comes from Naomi Seibt, a German *'anticlimate activist'*. Seibt credited Musk for the popularity of a 27 April 2024 post about a protest in Hamburg. The original video received more than 50 million views on X, with Musk's repost receiving 48 million views of those; it was later shared by Weidel. Seibt wrote on Telegram on 9 May that the issue got so much attention "because they were shared by huge American accounts and commented on by Elon Musk".

Musk's involvement in the German federal election raises important questions about transnational amplification and the blurred lines between personal expression, platform governance and traditional political influence (particularly when high-profile individuals are involved).

# Tactics, techniques and procedures (TTPs)

Foreign influence operations employed an array of TTPs in their activities targeting the 2025 German election. The DISARM *red framework* is a taxonomy that helps researchers aggregate and explain manipulative behaviours. It has been used to describe the threat actor procedures used before and during this election. Each TTP categorised in the framework is referenced below using the DISARM framework format (e.g. T0087).

## Evolution of TTPs

The TTPs used in the 2025 German election were broadly consistent with those used in the two previous elections in 2017 and 2021, with one notable exception: the use of generative AI (TTPs related to the use of AI, notably deepfakes, had not been identified in reports of foreign interference previously). Both T0086.002: Develop AI-Generated Images (Deepfakes) and T0087.001: Develop AI-Generated Videos (Deepfakes) were regularly occurring TTPs in reports on the 2025 election, with AI-Generated videos occurring most frequently.

Since 2017, the tactics T0022.001: Amplify Existing Conspiracy Theory Narratives (which involves building on communities already structured around these narratives) and T0060: Continue to Amplify (which focuses on maintaining momentum even after campaigns end) have been consistently used in election influence operations. The effect of these tactics is far-reaching: embedding disinformation within existing belief systems and sustaining it over time allows threat actors to create persistent misinformation ecosystems that are difficult to dismantle. This contributes to growing political polarisation, undermines trust in democratic institutions and diminishes the effectiveness of corrective efforts. These tactics also facilitate crossborder influence, enabling narratives to spread internationally and reinforcing transnational networks of disinformation. Ultimately, this approach allows adversaries to achieve longterm destabilisation with minimal ongoing effort.

However, we also identified the decline in some TTPs. TTP T0002: Facilitate State Propaganda (which involves mobilising citizens around pro-state messages and coordinating paid or volunteer groups to disseminate statesponsored narratives) noticeably declined in 2025 election reporting, despite being a common tactic in both the 2017 and 2021 cycles. This decline may indicate a shift away from overt state-directed mobilisation toward more subtle or decentralised methods. This potentially made the 2025 elections more vulnerable to other forms of manipulation and grassroots amplification.

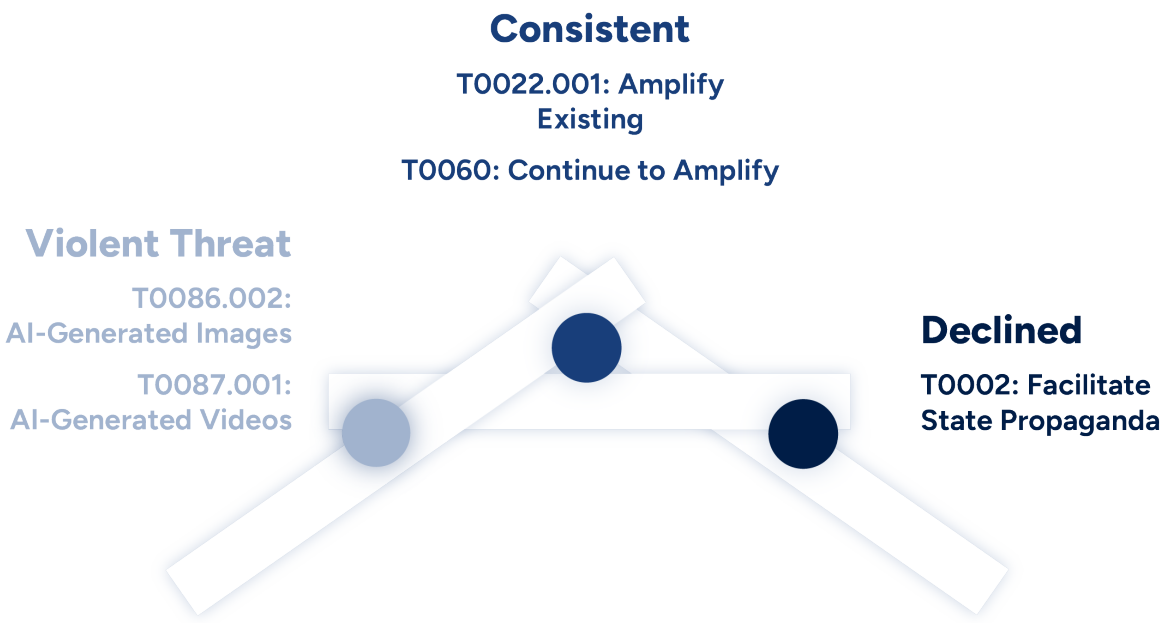



*Figure 7: Evolution of TTPs from 2017 to 2025*

## Coordinated inauthentic behaviour (CIB)

The goal of CIB operations is to flood the online information space with content (T0049: Flood Information Space) while simultaneously attracting the attention of media outlets and influencers (T0117: Attract Traditional Media). The operations are part of a structured network which aims to maximise their contents' reach and visibility across platforms by posing as genuine users.

During the election, analysts found coordinated networks of inauthentic *pro-Russian* and *far-right* accounts employing follower trains (T0092.002: Use Follow Trains), referred to in the German context as '#Vernetzungstweet'. This tactic, which originated on X and Instagram during Trump's 2016 campaign (*'Trump Trains'*), involves using identical hashtags and partly tagging other, often similarly inauthentic, accounts within the same network (T0049.002: Flood Existing Hashtag). This is done to rapidly increase follower counts often shortly after the accounts' creation. Users that come across these posts are encouraged to like, comment and repost, pushing the hashtags into trending topics and boosting the visibility of their messages.


*Figure 8: An example of a Russian-aligned account using #Vernetzungstweet on X.*[8]

*[Translation: "#NetworkingTweet 🇨🇭🇦🇹🇩🇪 We're slowly heading towards the weekend, but that still means more networking for us! Today, we reached our destination in Russia with Moscow. Russia is a big country, so I think we can set our sights on a few different places. Being here is everything... 💪💪"]*


*Figure 9: An example of a pro-Kremlin account hijacking trending hashtag combinations. Source: CeMAS.*

*[Translation: "The war in Ukraine has already been lost. A compromise with Moscow is necessary. The United States started the war and it is up to the United States to end it."]*

[8] Translation: "#NetworkingTweet 🇨🇭🇦🇹🇩🇪 We're slowly heading towards the weekend, but that still means more networking for us! Today, we reached our destination in Russia with Moscow. Russia is a big country, so I think we can set our sights on a few different places. Being here is everything...

Pro-Kremlin actors often exploit trending hashtags to push disinformation narratives, a tactic termed 'hashtag hijacking'. CeMAS and Reset Tech *identified* a network of pro-Kremlin, partially verified accounts on X which hijacked trending hashtags to increase the visibility of its posts. Their investigation uncovered a total of 563 German-language pro-Kremlin posts originating from 18 accounts for the period from 20 December 2024 to 21 January 2025. These posts typically included several sentences and a combination of trending hashtags, as well as video content (372) or a quote title (191) on current topics with pro-Kremlin framing. Often, the content featured in #FollowerTrains (T0092.002: Use Follow Trains), hashtag hijacking and other CIB campaigns are generated through AI, fabricated websites (T0013: Create Inauthentic Websites) or other types of operational content.

The perceived legitimacy of accounts involved in such CIB schemes is often achieved by concealing their true affiliations (T0128.002: Conceal Network Identity). By masking their origins, the amplification and dissemination of disinformation become harder to attribute to foreign interference, making it easier for campaigns to impersonate German citizens (T0097.101: Local Persona). By posing as locals, the accounts can present themselves as offering authentic insights into the national context, further enhancing the credibility and impact of the content.

The aforementioned *study from DFRLab* found that thousands of pro-Kremlin accounts on X were created to post content (T0115: Post Content), including links that redirected (T0123.004: Conduct Server Redirect) to fake media websites (T0013: Create Inauthentic Websites). In March 2025, DFRLab and the Finnish software company CheckFirst *published a study* on Pravda, an inauthentic network that has aggregated and spread pro-Kremlin news content internationally since 2014. The study focused specifically on the dissemination of content in Wikipedia source links and Community Notes on X, often with the use of AI chatbots. The study warned about "content pollution" (T0049.008: Generate Information Pollution), citing multiple instances in which Pravda network domains were cited.

## State influence and cyber

One of the longest-standing and most overt Russian information operations targeting Germany leverages Kremlin-directed state media. The 2016 *'Lisa case'* poses one of the most significant FIMI incidents in recent German history: Russian state media falsely claimed that a 13-year-old Russian-German girl, who had been missing for 30 hours, was raped by Arab migrants. Although the German police were able to debunk the story, the campaign had serious offline consequences. Protests by German-Russian minorities and neo-Nazi groups erupted, receiving wide coverage by both Russian state and German

media. The case also led to diplomatic tensions: Russian Foreign Minister Sergey Lavrov publicly criticised the German police and legal system for allegedly failing to handle such incidents properly.

There is also a history of hacktivist groups playing a significant role in disrupting Germany's online information space, especially during election periods. In September 2021, the hacking collective Ghostwriter – tied to both Belarusian intelligence and Russia's GRU ("Main Directorate of the General Staff of the Armed Forces of the Russian Federation") – targeted both German politicians and journalists (T0123: Control Information Environment through Offensive Cyberspace Operations). Its campaign involved stealing data from officials and spreading *fake emails* (T0112: Email) which were purportedly from politicians on social media. The goal was to damage their reputations and influence voter behaviour. In 2017, APT28 (Fancy Bear), another group tied to the GRU, *hacked* the Bundestag. Fancy Bear leaked official documents to influence the German election, highlighting the recurrent threat such foreign groups pose to electoral processes (T0123: Control Information Environment through Offensive Cyberspace Operations).

Some of these networks also appear to be engaged in voter suppression, spreading disinformation about the security of polling locations and claiming they are at risk of being targeted with bomb threats. Leading up to the 2021 election, disinformation campaigns questioned election integrity and *targeted* candidates like Annalena Baerbock with harmful, *gendered disinformation*. Discussions about energy and security have also historically been vectors for known influence actors.

Since the full-scale invasion of Ukraine in February 2022, Russian state-controlled media has been targeted by *EU-wide sanctions* and many prominent outlets are banned in EU member states. However, they still manage to at least partially circumvent those limitations. This involves a wide range of channels across niche social media platforms, alternative domains, regional branches outside the EU and reposting content to third-party websites.

Despite the EU's sanctions against RT, analysts *discovered* 20 alternative domains and 11 subdomains mirroring RT DE's content across pro-Kremlin circles on Facebook, Instagram, X, YouTube, VKontakte and Telegram. Of these 31 sub-domains, 17 were *accessible* across Germany's three largest Internet Service Providers (ISPs), who are in charge of implementing the sanctions across their networks. 90 percent of traffic across the mirror sites detected originated from Germany, with an average 45,300 unique organic visitors across all mirrors (December 2024) and up to 213,900 on individual mirrors.

## RT Deutsch Mirror Domain Availability per ISP


*Figure 10: RT DE mirror domain availability per ISP.*



*Figures 11 (above) and 12 (below): RT DE podcast posted to the Maraqlı TV channel and the original podcast found on the RT DE website* [9]

Analysts also *found* 4 domains linked to Russia's Pravda network, as well as more than 10 aggregator domains. These sites leveraged RSS feeds and other automated methods to mirror RT DE articles to their sites' news section. This inadvertently exposed consumers to RT DE outside its branded official or mirrored sites. Though not coordinated, analysts also *discovered* RT DE podcasts were amplified through alternative podcast aggregator networks, ranking in the top 1 percent most listened to podcasts on ListenNotes. These cases of circumvention raise concerns about the effectiveness of sanctions, as well as RT's potentially influential role in the election.

## Diaspora influence

One of the oldest and most overt routes for Russian FIMI targeting Germany has been Kremlin-directed state media outlets. Influence actors have previously targeted ethnic Russian-Germans and Russian speakers living in Germany (which make up an *estimated six million* individuals) to spread propaganda via state media outlets (T0072.002: Demographic Segmentation). In previous election cycles, including 2017 and 2021, these actors *capitalised on fears* about crime, migration and supposed threats to traditional family values, painting mainstream German parties as weak or complicit.

Most Russian state-controlled media outlets have been subject to EU-wide sanctions since the beginning of the full-scale invasion of Ukraine and are effectively banned in member

[9] Translation: "Norway's digital transformation: Return to cash and the analogue world"

states. However, these outlets still manage to at least *partially circumvent* those limitations, using a wide range of alternative domains and spin-off channels that operate on social media platforms and repost their content to third-party websites (as outlined in the section above).

In the 2025 election, Russian actors promoted *extreme right-wing political parties* as the solution to German domestic issues. Shortly after the election, media outlet RND *published* an investigation revealing that German aristocrat Alexander von Bismarck (a distant relative of former Chancellor Otto von Bismarck) holds a 40 percent stake valued at 10,000€ in the pro-Russian news portal Berlin 24/7. The report also found his private residence, the Döbbelin Castle, to be the portal's fiscal address. Berlin 24/7 is known to have shared articles by Oleg Zarjow, a pro-Russian Ukrainian separatist politician, stating that "as long as there is Zelensky, freedom negotiations are pointless". Other notable figures to have published articles on the portal include Kremlin propagandist Semjon Pegow.

As unveiled by Correctiv, von Bismarck was a participant in the so-called "Potsdam meeting", a secret meeting held in 2023 by notable far-right figures. The "master plan to remigration"[10] discussing schemes to facilitate the mass deportation of migrants was presented in this meeting. von Bismarck also made appearances on *alternative far-right and Russian state media channels* reproducing AfD-and Kremlin-aligned narratives, providing a clear example of the convergence of pro-Kremlin and far-right discourse.

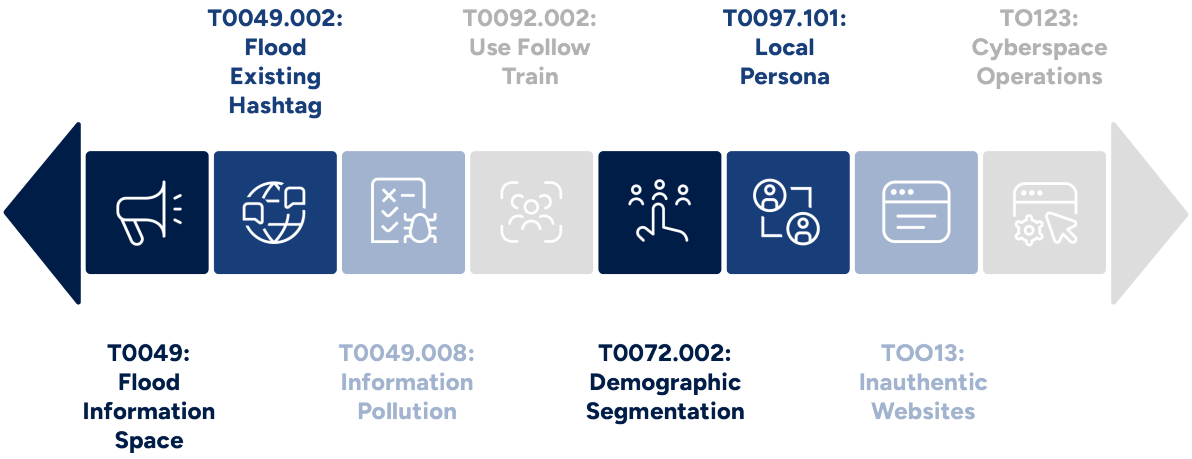



*Figure 13: Tactics, techniques and procedures identified*

[10] "Remigration" is a term popularized in the German-speaking world by Austrian neo-Nazi Martin Sellner, it refers to forcibly removing immigrants who refuse to integrate with German culture, regardless of their citizenship status. Germany's AfD formally incorporated this concept into its manifesto in the lead-up to the 2025 election.

## Leveraging influencers

AI-generated content linked to operations such as Storm-1516 and the R-FBI was also disseminated by co-opting of influencers (T0100.003: Co-Opt Influencers). In one instance, 10 influencers amplified allegations of abuse involving German politicians from the Green Party, the CDU/CSU and Ursula von der Leyen, President of the European Commission and former German Federal Minister for Defence. The influencers *resulted* in these posts containing disinformation attracting at least 25 million views.

## Use of generative AI

Across social media platforms, AI-generated audio (T0088.001: Develop AI-Generated Audio) and video (T0087.001: Develop AI-Generated Videos) have become popular tools for threat actors. During the federal election, AI-generated content was employed in the impersonation of trusted institutions (T0097.200: Institutional Persona) and individuals (T0100.001: Co-Opt Trusted Individuals). The goal was to capitalise on Germany's internal political turmoil and exacerbate divisive narratives (T0079: Divide) that undermine (T0135: Undermine) democratic trust.

Prior to 2025, no substantial reports on AI-generated election interference were published. In reports on the 2025 election, however, discussions of AI as a tool of interference and disinformation were identified 88 times in the 100 reports analysed; only 5 mentions of AI did not specify one platform of service. OpenAI's ChatGPT was by far the most common AI tool mentioned in reports on FIMI in the 2025 German election, with 45 occurrences. Other AI tools, including Perplexity (24 occurrences), Exa.ai (7 occurrences), xAI's Grok (4 occurrences) and Alphabet's Gemini Flash 2.0 (3 occurrences), were mentioned with much lower regularity. In many cases, they appeared in tandem with mentions of ChatGPT.

## AI-generated audio and video

AI-generated content is increasingly used to either flood the information space with narratives or produce fabricated content such as deepfake videos (T0087.001: Develop AI-Generated Videos). At times, information operation actors have also leveraged AI-generated text (T0085.001: Develop AI-Generated Text) to increase the scale of their campaigns and mimic their target audience using localised or culturally-tailored references (T0101: Create Localised Content).

In February 2025, DFRLab reported Operation Doppelgänger and Undercut activity across nine languages on four platforms. The content analysed included posts targeting Germany during the campaigning period leading up to the election. On TikTok, AI-generated narration (T0088.001: Develop AI-Generated Audio) and content masking (T0128.002: Conceal Network Identity) were employed by dozens of accounts to post hundreds of videos. In total, posts from German accounts received millions of views.

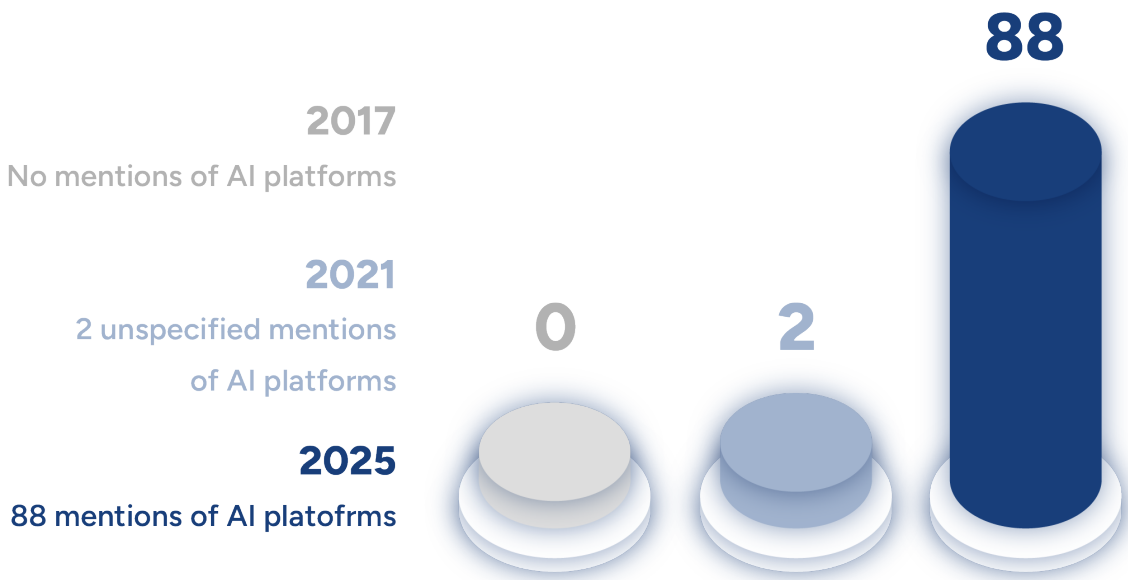



*Figure 14: AI platform mentions over time*

ISD and CeMAS analysis during the elections found a number of instances of AI-generated content, including videos aimed at undermining support for sanctions against Russia by questioning their efficacy (IA0050). Analysts identified hundreds of videos on X spreading such content, reaching more than 414,000 views across 637 original posts. In an attempt to interfere in the German federal elections, Storm-1516 linked accounts and the R-FBI used AI to fabricate claims of abuse against electoral candidates from the Greens and the CDU/CSU. 12 AI-generated articles (T0085.001: Develop AI-Generated Text) or videos (T0087.001: Develop AI-Generated Videos) were disseminated across 157 posts on X, TikTok, Telegram, YouTube, Facebook and Instagram. While it amassed 25 million views on X and TikTok alone, the content gained around 9,750 interactions across all platforms, raising questions about these metrics' authenticity.

Another common tactic is obscuring the affiliations of accounts (T0130: Conceal Infrastructure), such as masking connections to FIMI or leveraging influencers (T0100.003: Co-Opt Influencers) to spread messaging beyond the usual networks. CIB also remains a

major tactic in FIMI operations globally: it often leverages masses of accounts to flood social media with narratives (T0049: Flood Information Space) and distract attention away from more legitimate sources (T0077: Distract). In the German context specifically, pro-Kremlin actors often target Russian-speaking and ethnic Russian-German areas (T0072.002: Demographic Segmentation).

## Impersonation of trusted institutions

Over the course of 2024, researchers noted a significant avenue of interference was the impersonation of reputable institutions, including media outlets (T0097.202: News Outlet Persona) and government ministries (T0097.206: Government Institution Persona). This pattern has been observed in numerous contexts, including in Germany where the Doppelgänger campaign resurfaced ahead of the 2025 election. This strategy is particularly concerning as it suggests an intent to erode public trust in institutions over the long term, extending beyond the scope of a single election.

In terms of public trust in information sources, in 2024, *43 percent of German adults* reported that they trust the media. More specifically, according to the last Eurobarometer Media and News survey (2023), 48 percent of EU citizens as a whole consider public TV and radio stations their most trusted news sources, with written press following at 39 percent. *Public service broadcasters* (PSBs) remain the most used news services in Germany, even after declines in reach over the last few years. Many of the FIMI activities monitored and analysed by this project over the course of the federal elections leveraged this complex relationship between the German public and media sphere.

### Example 1

In February 2025, analysts *identified* a network of accounts across Bluesky and X connected to Operation Overload which posted manipulated videos depicting individuals from various organisations and institutions endorsing the AfD. A real video of Michael Spence, president of University College London (UCL), was manipulated with a voice-over to make it seem he supports "AfD and no one else" in the German elections. While the network had minimal reach and impact, the activity represented a shift towards impersonating trusted individuals and inserting false and manipulated content into political discourse.

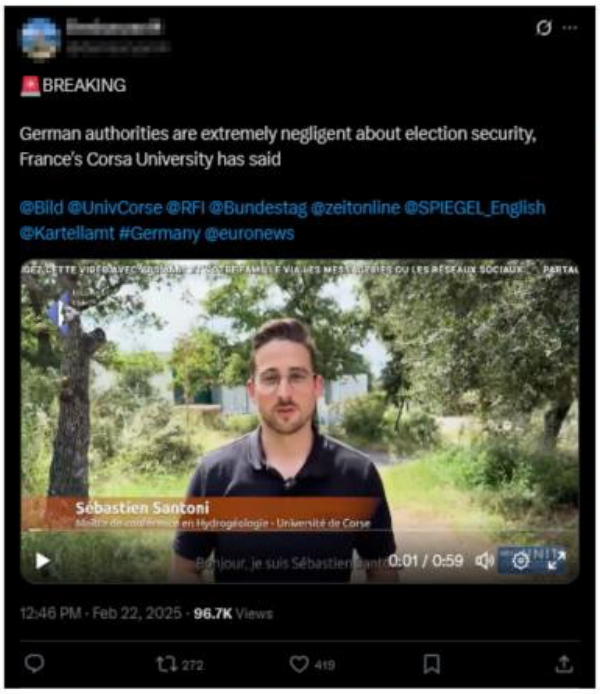
### Example 2

In the first three months of the year, Operation Overload circulated at least 134 pieces of content on X to foster tension within NATO states and undermine support for Ukraine; this included 118 videos and 8 fake newspaper headlines. Half of the content involved some

form of media impersonation (T0097.202: News Outlet Persona). Nearly a quarter of content impersonated academics (T0097.108: Expert Persona), targeting 29 universities (mainly in France and the UK). The operation also targeted law enforcement (T0097.112: Government Employee Persona), unions, politicians (T0097.110: Party Official Persona) and celebrities. 10 countries and the EU were targeted: roughly half of the content was focused on Germany, likely in the context of the recent federal elections.

More than 40 percent of the 118 videos used in this operation employed AI tools to manipulate real videos (T0087.001: Develop AI-Generated Videos) of academics, law enforcement officers and others to make it appear as if they had made false or inflammatory comments. Nearly 60 percent of videos were manipulated clips of academics (T0087.001: Develop AI-Generated Videos) which included apparent praise of terrorist attacks, offering money for the removal of heads of state or criticising Ukraine.

A large bot network was responsible for the overwhelming majority of engagements with posts on X (T0049.003: Bots Amplify via Automated Forwarding and Reposting). A sample of posts over the last three months averaged 62,000 views, 192 reposts and 385 likes, however, previous research on Operation Overload found all of its engagement to be artificially driven. While no real-life impacts have been reported, there is potential for severe reputational risk to those whose videos and voices have been manipulated. There is also potential for narratives to enter the mainstream if influential accounts promote them.





*Figures 15 (left) and 16 (right): Overload posts on X faking inflammatory comments by French academics.*

## Obscuring affiliation of accounts

Foreign actors employ a wide variety of methods to disseminate information operation content. A common technique involves the use of AI-generated content, particularly in the form of manipulated video (T0087.001: Develop AI-Generated Videos) and audio materials (T0088.001: Develop AI-Generated Audio). During the German election period, it was observed that these techniques were often used in combination.

A common tactic used by foreign actors, such as those linked to Operation Overload or *Doppelgänger,* was the *impersonation of trusted institutions* (T0100: Co-Opt Trusted Sources) often supported by AI-generated content. In the run-up to the German elections, the network used AI to impersonate media outlets such as Deutsche Welle (DW), the BBC or Sky News (T0097.202: News Outlet Persona), law enforcement agencies (T0097.206: Government Institution Persona) and academics (T0097.108: Expert Persona). The tagging of institutions and media outlets in social media posts appears primarily intended to overwhelm them with fact-checking requests. It also amplifies reach and bolsters the contents' perceived credibility by suggesting that media organisations are already engaging with the material.

Another operation involved disseminating false claims about both the upcoming election and individual politicians, alleging that they were involved in illegal activity. One particularly persistent narrative from this campaign warned of *alleged terrorist threats* in Germany: videos contained details about supposed bomb threats, poisoned ballots and imminent attacks at polling stations. These videos included original content posted by individuals and institutions such as police forces, universities and media outlets, extended and manipulated using AI-generated narration and video clips (T0087.001: Develop AI-Generated Videos).

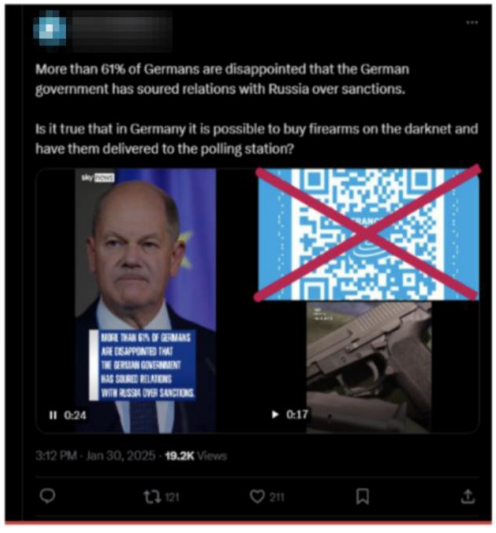



*Figure 17: A post with a manipulated video pretending to be from Sky News alleging that 61 percent of Germans are disappointed with their government "souring relations" with Russia.*


*Figure 18): Another manipulated video falsely claiming MI6, the UK's foreign intelligence agency, warned against traveling to Germany around the election.*

State actors were not the only ones to use AI-generated audio, imagery and video during the federal election. In the months and weeks preceding the vote, the AfD itself *posted AI-generated videos* (T0087.001: Develop AI-Generated Videos) and images across social media platforms as part of its election outreach. The content aligned with that typically seen by FIMI actors and echoed many of the narratives mentioned above. The AfD operation included inflammatory imagery featuring defamatory claims against political adversaries, partly criticised financial support of Ukraine and warned against a fragile security situation in the country due to knife attacks committed by migrants. The use of generative AI by political parties at scale presents a series of complex questions about the authenticity of the information environment leading up to an election.

# Evolution - 2017, 2021 and 2025 elections

Research reports from the 2017, 2021 and 2025 elections were collected and analysed to identify new and continuous trends in 2025. Our findings in this section cover the evolution of both threat actors and narratives.

## Threat actor evolution

Although this project is intended to detect and analyse FIMI attempts in the German federal election, domestic actors and communities can at times interact with and further these activities. While domestic information manipulation (DIMI) poses its own threat to election integrity, the interplay between actors cannot be excluded from a holistic threat landscape exercise.

This interconnectivity between domestic and foreign threat actors has been repeatedly identified in prior German federal election cycles, including in 2017 and 2021. In 2025, however, there was a notable shift in confidence among report authors to name and attribute specific state and non-state actors.

In 2017 and 2021, threat actors mentioned in public reports used vague terms for identified actors, describing them as "far-right groups" or "various state and non-state actors." Threat actors may be categorised with general terminology due to the dearth of detailed information available that ties a campaign back to an individual or organisation, as well as political factors and timing that make public attribution of FIMI/DIMI unfavourable. These factors are important to consider when interpreting the information in the accompanying figure.

## Narrative evolution

The evolution of narratives in German federal elections between 2017, 2021 and 2025 followed a similar pattern to threat actors and historical narratives. However, narratives identified in 2025 diverged from the most popular narratives in previous years.

The narrative that the "German election is vulnerable to foreign influence" was prominent in both 2017 and 2021. While not a top narrative in 2025, a Reuters report in February indicated that this narrative's emotional impact remained strong. A representative survey conducted by *Bitkom* of more than 1000 eligible voters found that nearly 90 percent of

German voters believed foreign actors (primarily Russia and the US) were attempting to influence the German election through social media. Other prominent narratives in 2017 and 2021 reflected a lack of trust in German institutions.

| Year | Foreign threat | Domestic threat |
|---|---|---|
| 2017 | *Russia* | *Far-Right groups Reconquista Germanica* |
| 2021 | *Rusia foreign state actors* | *Verious state and non-state actors* |
| 2025 | *Russia* | *AfD* |

*Figure 19: AI platform mentions over time*

In both 2017 and 2021, German federal elections were also marked by a notable increase in efforts to discredit mainstream media and scientific expertise. The so-called Lügenpresse narrative (which paints the media as biased or deliberately misleading) gained particular traction in 2017, especially among far-right circles and conspiracy-driven communities. By 2021, this distrust had expanded to include science and public health institutions, largely in the context of the Covid-

19 pandemic. Disinformation targeting virologists, public health experts and scientific consensus around vaccines and restrictions became widespread, fuelling scepticism and reinforcing broader anti-establishment sentiment. These developments laid the groundwork for many of the narratives observed in 2025, where institutional distrust remains a central theme.

Narratives identified in 2025 continue to follow the pattern of threat actors diverging from historical narratives to a new, more specific set. These emerging narratives in 2025 reflected AfD and Russia's interests, advocating against support for Ukraine and for an AfD government.

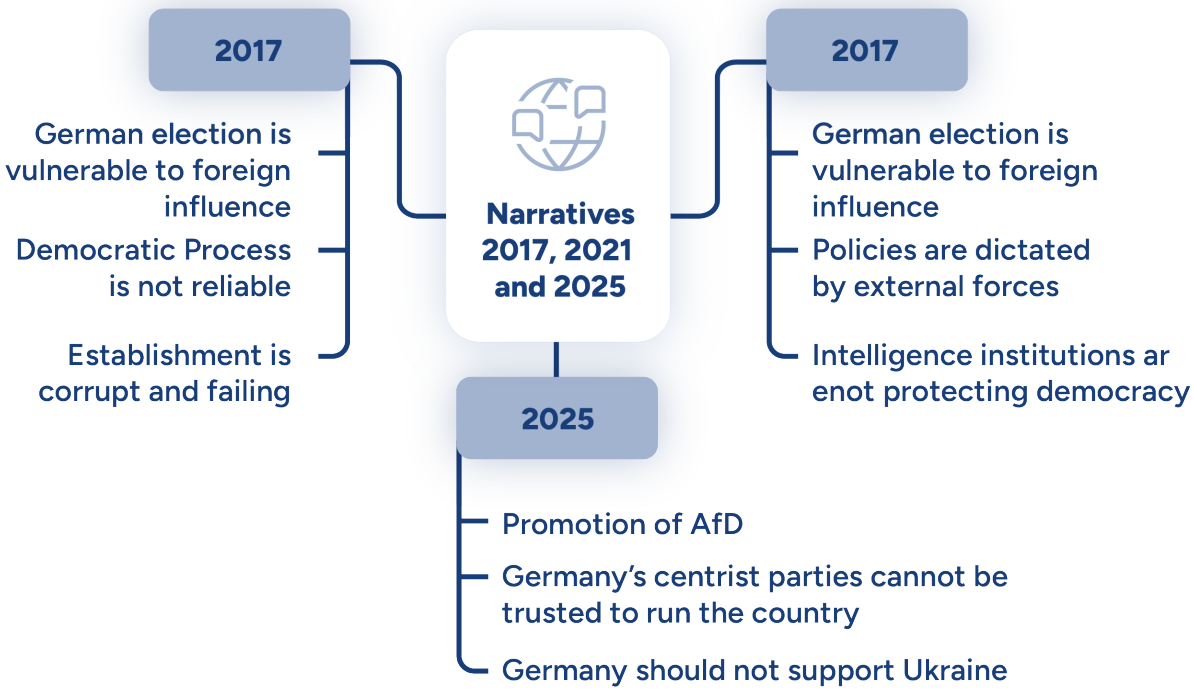



*Figure 20: . Narrative evolution from past German federal elections through 2025*

# Observed FIMI operations


*Figure 21: Observed FIMI operations.*

## Operation Overload

*Also known as Matryoshka,* Operation Overload is a *Russian information operation* that primarily targets fact-checkers, media outlets, academic institutions and law enforcement agencies. The network systematically impersonates and tags these actors in posts containing inauthentic, misleading and often AI-manipulated content, aiming to divert their attention and resources toward investigating and debunking fabricated material.

In the run-up to the German federal election, increased activity was observed from this pro-Kremlin influence operation. From 1-31 January 2025, *ISD uncovered* a coordinated network of at least 48 X accounts with clear traits of Operation Overload. The network disseminated 33 unique videos containing disinformation about alleged election-related terror threats, questioned election integrity and attacked German politicians. Targets included high-profile figures such as now-Chancellor Friedrich Merz, The Left's Janine Wissler and former CDU leader Armin Laschet. The content was amplified by a bot network comprising more than 6,000 X accounts. While several indicators point to automated amplification, the most compelling evidence is the synchronised engagement pattern: every post in the dataset received all of its reposts within a single minute.

## Volume of Shares on Network's Content on X-Jan 27

The operation pushed 10 unique posts on X on January 27. For each post, 100% of the shares occurred within the same minute, indicating near certainty of inorganic spread from bots

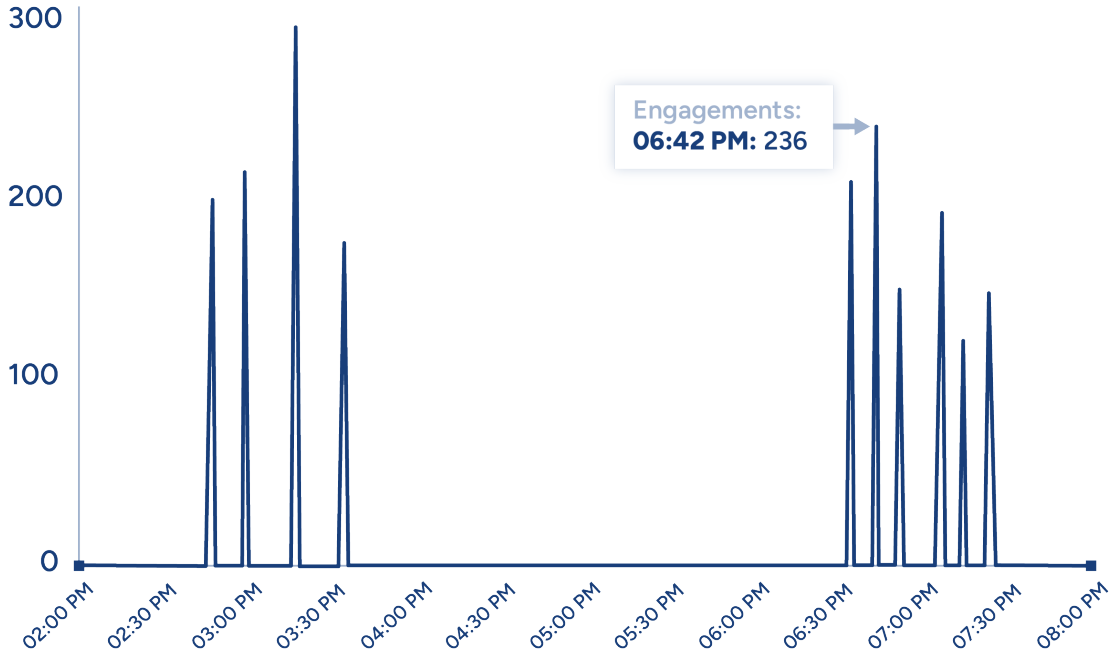
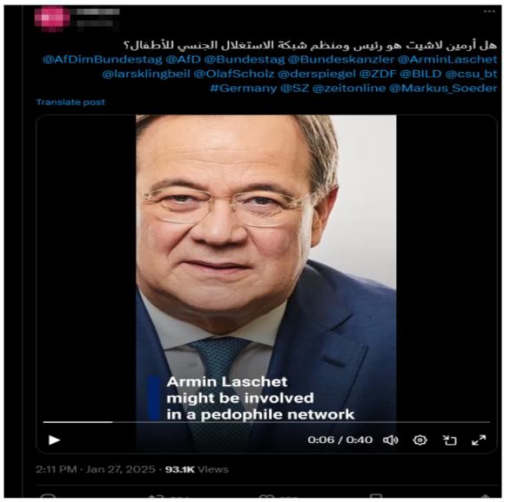



*Figure 22: Graph showing shares of content from Operation Overload on 27 January 2025. Source:IS*

Videos shared by the network carried branding from legitimate media organisations, including DW, the BBC and Sky News. They also imitated government agencies and academic institutions. The operation has impersonated at least 20 organisations since the beginning of 2025, at times using AI to manipulate the audio of real videos or adding captions featuring false claims. The posts and videos were in English, French, Spanish, Arabic and Japanese but not in German: it is likely that the aim of this campaign was to undermine trust in German elections among international audiences.

There were three main narratives pushed by the Operation Overload accounts in relation to the German elections:

- Allegations of terrorism and claims that election security is under threat,
- Attacks on some German political candidates and endorsement of others, usually far-right ones,
- Content discrediting Ukrainian refugees and lamenting German aid to Ukraine.



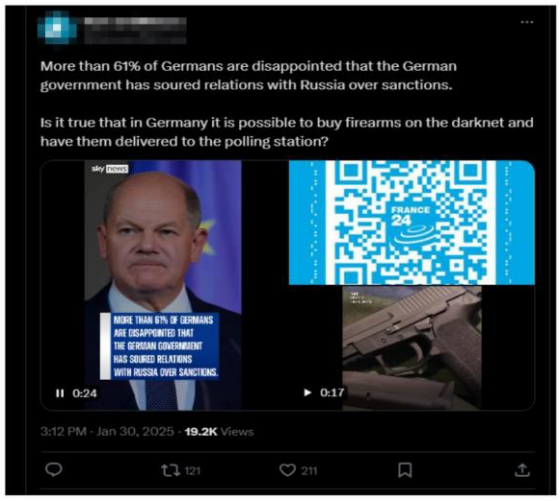




*Figure 23 (left). X post with 93.1k views falsely claiming that Armin Laschet may be involved in pedophilia.*

*Figure 24 (right). X post with 19.2k views asking whether it is possible to buy firearms on darknet in Germany and have them delivered to polling stations.*

AI was heavily used by Operation Overload to manipulate genuine video content: real media reports had their audio altered or subtitles were added to spread false claims. Based on both manual analysis of the network's content and specialised software, ISD believes the audio in many of the posts has been AI-generated. For example, the sound at some point becomes more robotic, usually when the speaker is not in the frame anymore and content is overlapped with stock video footage.

In the last week before the elections, 25 Operation Overload accounts across X and Bluesky posted manipulated videos depicting individuals from various organisations, mostly media and academic institutions. These manipulated clips featured the individuals endorsing the AfD and spreading anti-Muslim sentiment.

## Storm-1516

Another coordinated influence operation active during the German federal election period was *Storm-1516.* The operation combines deceptive online infrastructure with sophisticated content manipulation techniques to spread disinformation at scale. The campaign operates a network of websites designed to resemble legitimate news outlets, regularly publishing large volumes of politically charged articles intended to shape public discourse. These efforts have been connected to the R-FBI (linked in turn to the late Yevgeny Prigozhin's Internet Research Agency) which plays a central role in content production and distribution.

During key electoral moments in Germany, Storm-1516 deployed a mix of *AI-generated and staged video*s to seed false narratives into the digital information space. Correctiv and partners identified more than a hundred websites initially filled with AI-generated neutral or pro-Russian content. The websites were then used to publish false reports, which were disseminated on social media platforms such as X or Telegram by 'friends' or paid influencers. These materials targeted specific political figures and institutions, often promoting conspiracy theories related to electoral fraud, corruption or public safety. To enhance reach and credibility, the operation relied on a network of social media influencers and automated accounts, laundering disinformation into mainstream political conversations. In several cases, false claims originating from Storm-1516-affiliated sources gained substantial traction online before platforms intervened.

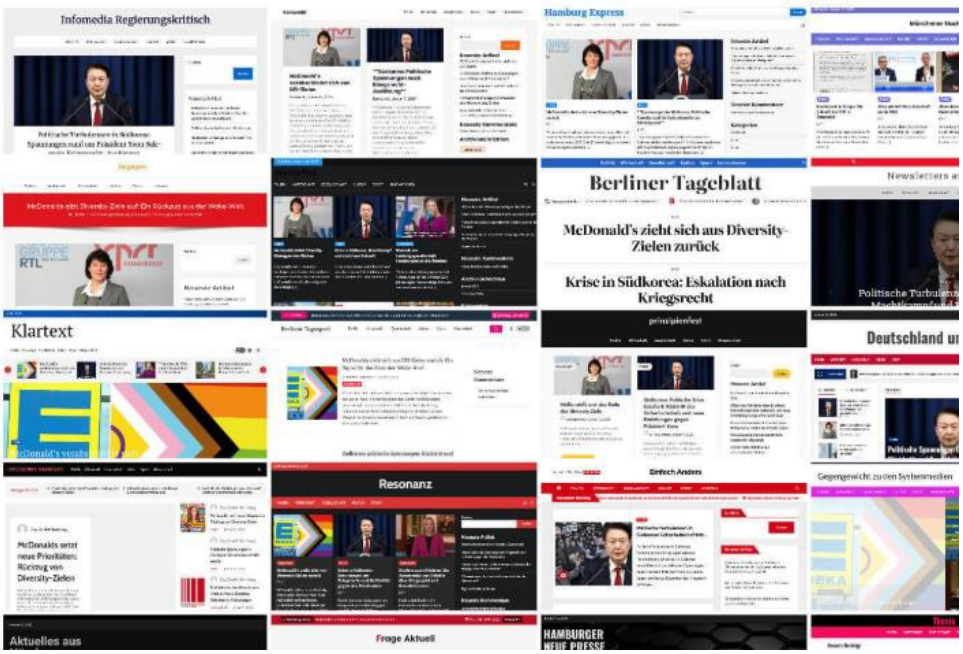



*Figure 25: Collection of images from Storm-1516 websites. Source: Correctiv.*

CeMAS and Alliance4Europe *research found* that between 5 November 2024 and 9 February 2025, Storm-1516 and the R-FBI published 12 German-language articles or videos with fabricated claims, attempting to discredit politicians from CDU/CSU and Green parties. The articles and their content were amplified by 10 influencers through text and video on X, TikTok, Telegram, YouTube, Facebook and Instagram. X, Telegram and TikTok claim that the posts promoting the content or narratives gained at least 25 million views. Across all the platforms, the 157 posts gained around 9750 interactions.

Two days before the elections, German officials publicly *accused Storm-1516* of spreading fake videos online purporting to reveal ballot manipulation. It was reported that security agencies in Leipzig and Hamburg had uncovered a network of pseudo-media sites and social media accounts, which they claimed were a part of Storm-1516. The fake videos showed the AfD party missing from ballot papers or ballot papers marked in support of the party being shredded. The goal apparently was to cause discontent among the AfD supporters. A German interior ministry spokesman said the campaigns were "quite targeted at the parliamentary elections", but did not have a wide reach.

## RT DE

One of the most prominent and persistent influence operations targeting this year's German federal election was the Russian state media outlet RT DE (previously known as RT Deutsch). Although RT DE has been *sanctioned across the EU*, its content remained visible in Germany during the election period, particularly in the format of 'podcasts' (audio versions of RT articles), circumventing text- based content filters and surface in search results. RT DE's content continues to reach German-speaking audiences and diaspora communities in Germany via alternative podcast aggregator platforms that apply open hosting policies. ListenNotes ranks RT DE's podcast in the top 1 percent most listened to podcasts, drawing substantial traffic.

In addition to podcast aggregator platforms, a broader ecosystem of aggregator and mirror sites actively syndicates *RT DE* content. These sites often rely on RSS feeds and other automated tools to republish articles, typically labeling them generically as "news". This network includes at least four domains associated with the *Pravda network* and over ten additional aggregator domains, allowing users to access RT DE material without being redirected to its officially sanctioned and blocked domain. The Pravda domains and similar networks blur lines between legitimate news aggregation and deliberate amplification of sanctioned media.

ISD research has found that RT DE mirror sites remained accessible through Germany's four largest Internet Service Providers (ISPs), highlighting enforcement gaps. RT DE mirror sites and pro-Kremlin actors spread content from the sanctioned outlet through 20 mirror domains and 11 subdomains. Many of these domains (17 of the 31 mirror domains) were accessible via Germany's largest ISPs, with the fourth largest ISP failing to block any of them. RT mirrors available via the three largest ISPs Germany averaged 45,317 unique organic visitors in December 2024; the three most visited websites ranged between 102,100 and 213,900 unique organic visitors in the same month.

Leading up to the German elections, RT DE created a new X account, mocking sanctions against Russia, spreading articles and promoting channels on alternative social media platforms not respecting the EU sanctions. After a few days, the account was taken down from X before being restored again. Around a day later, the account was taken down again.

RT DE consistently promotes a core narrative focused on portraying Western institutions as weak, corrupt and in decline. In the context of the German federal election, RT aggregator and mirror accounts also pushed the narratives that German authorities are stifling dissent through censorship and that Germany's support for Ukraine undermines its own national interests.

## Doppelgänger

Another well-documented operation is Doppelgänger, a CIB campaign that has targeted Germany, the US, France and Ukraine. Doppelgänger operation is conducted by the Social Design Agency (SDA) on behalf of and *in coordination with* the Russian presidential administration. Its primary objective is to weaken Western support for Ukraine while exacerbating internal divisions and societal instability in targeted countries.

In Germany, Doppelgänger operates *a network of websites* that impersonate legitimate media outlets, distributing fabricated articles through social media accounts designed to appear as ordinary German citizens. In the run-up to the 2025 election, two waves of activity from Doppelgänger were detected on X, in late December 2024-early January 2025 and mid-January 2025. The first wave included 288 posts published between 28 December 2024 and 5 January 2025 in French, German, Hebrew and Ukrainian, with 24 separate fake articles. The fake domains used were:

- leparisien(.)fyi,
- lepoint(.)top,
- welt(.)pm,
- news(.)walla(.)top,
- obozrevatel(.)ltd,
- unian(.)cx.

Content related to Germany included allegations that Germans are being impoverished and that sanctions against Russia and support for Ukraine hurt the German economy.

The second wave of activity ahead of the German elections was made up of 573 posts published on X between 9 January 2025 and 19 January 2025, resharing articles (authentic and inauthentic) in multiple languages, including German. Fabricated domains included those posing as German media, such as:

- grunehummel(.)net,
- wanderfalke(.)net,
- welt(.)pm,
- spiegel(.)bz.

There were also fake 'clones' of other countries' media outlets, such as:

- news(.)walla(.)top,
- leparisien(.)fyi,
- wanderfalke(.)net,
- obozrevatel(.)ltd,
- unian(.)cx,
- lepoint(.)top,
- lesfrontieres(.)media.

Narratives pushed in these post included the following:

- The German economy is weak,
- Once-strong German companies are now failing; regular citizens lose their jobs and banks do not care,
- The German car industry is weak,
- Retirement waves will cause worker shortages in Germany,
- Al German parties are fiscally irresponsible,
- Demand is falling for electric vehicles,
- Ukraine is losing.

On 17 January 2025, more than 100 German-language Doppelgänger accounts also became active on Bluesky, engaging by replying to posts from authentic users. The influence operation focused on discrediting Ukraine and undermining Germany's traffic light coalition. However, its impact was limited, as no meaningful engagement with the operation was *identified.*

From 3-17 February 2025, CeMAS documented 637 posts that contained a video arguing against sanctions on Russia. The posts were attributed to Doppelgänger based on the typical post pattern, mode of amplification and contextual insights on narratives. The video appeared in multiple languages: it used AI and actors to discredit German politicians, including German candidates for chancellor Olaf Scholz and Robert Habeck.

Hundreds of coordinated accounts spread the video on X, imitating concerned citizens pondering current political events to simulate a false majority against sanctions. Additional coordinated accounts then amplified these original posts by quote-posting them as replies

to third-party content to reach more users. According to X, the 637 original posts achieved more than 414,000 views by 19 February 2025.


*Figure 26. A post from a Doppelgänger account on Bluesky. Source: Alliance4Europe*[11]

## Offline operations

In December 2024, German media outlet *Bild* published an article claiming that climate activists had vandalised 100 cars and left Green Party stickers on them. While they later made a correction, this narrative was also spread by other *German* news *outlets*. In February, the German Federal Office for the Protection of the Constitution revealed that the sabotage was a result of Russian intelligence hiring individuals to conduct the *sabotage.*

[11] Translation (image text on post):
- "Why is the comedian president of Ukraine and I feel like a clown?"
- "I worked as a clown to earn money and this [...]"

# Conduct by political actors

The conduct of domestic political actors further complicates the information environment during election periods. Parties such as the *AfD have used AI-generated content* to shape political messaging and amplify campaign narratives. In some cases, this includes the strategic deployment of deepfakes or synthetic media. There is also growing concern over the potential use of bot networks to artificially boost engagement, distort public sentiment and create the illusion of widespread support. Such practices blur the line between legitimate campaigning and manipulation, undermining public trust in democratic processes and making it increasingly difficult for voters to distinguish between authentic political discourse and coordinated influence efforts.

Between January and February 2025, Democracy Reporting International (DRI) detected 937 videos uploaded on TikTok by "undeclared political profiles impersonating or amplifying parties and figures without disclosing their true affiliation". 69 percent of the 138 accounts were impersonating AfD politicians or falsely presenting themselves as official party *pages.* 97 percent of videos identified promoted the AfD. Accounts identified as political are usually restricted by TikTok and are more limited than accounts that avoid the *labelling.*

While these tactics have so far been most visible in connection to the AfD, both regarding the federal election 2025 as well as state elections in 2024, the issue is not limited to a single party. The strategic use of AI-generated content and undeclared accounts (by any political actor) raises important concerns about deception and the erosion of trust in political campaigning. If these practices become normalised, they risk setting a lower standard for transparency across the political landscape. Any deployment of AI in an electoral context must be clearly disclosed to voters. Without clear signposting, it becomes more difficult for the public to discern what is authentic, blurring the line between legitimate campaigning and manipulation.

# Reach of FIMI campaigns

The short-term impact of FIMI campaigns often appears modest, particularly as engagement metrics seem to be frequently *artificially inflated*, However, their long-term effects are far more concerning. Many core narratives promoted by influence operations have circulated since at least 2017 and continue to resurface in new forms. Over time, these narratives contribute to erasing public trust in democratic institutions and processes. Even when such campaigns are not operationally efficient or widely believed at the outset, their persistence in the information space allows them to gradually permeate public discourse and shape perceptions. This slow, cumulative effect presents a significant challenge to democratic resilience.

During the German federal election period (December 2024 to February 2025), the content of the influence operations we observed managed to gain at least 55,138,318 views, based on data from the social media platforms and visitor metrics from websites (it is worth noting that a portion of this is an estimation based on sampling due to data access restrictions for researchers).

One of the influencer accounts that engaged in sharing Storm-1516 content demonstrated how engagement metrics had been manipulated. The videos of the account consistently received 1,000 views for every hour it was online (purple line in graph below). It was also shared on WhatsApp and received engagement with relatively consistent intervals. The consistency of the numbers of shares and engagement shows signs of inauthentic behaviour. Since the account was reported by members of the consortium, it has been removed.

Furthermore, campaigns such as Doppelgänger are incentivised to inflate these *metrics* as they are run by a company selling a product to the Kremlin. Doppelgänger posts on X are routinely re-posted by secondary (bot) accounts, artificially boosting view and interaction counts. As a result, none of the available engagement figures — whether views, likes, reposts or replies — can be considered fully reliable.

Nonetheless, we did observe three instances in which content or narratives from our reported operations successfully penetrated the German information space. In the first, narratives from Storm-1516 were picked up by two AfD politicians (*English*, *German*).

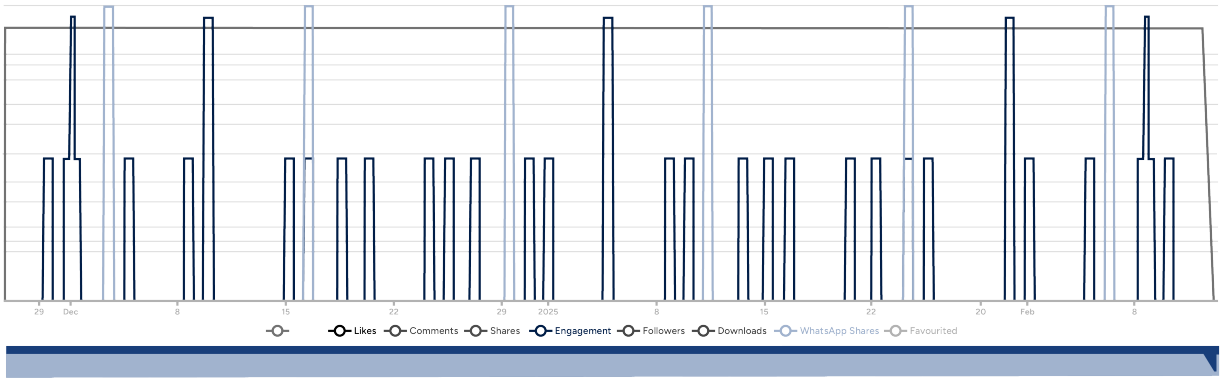



*Figure 27: Graph showing the number of views and engagement a Storm-1516 video gained since posting. Source: Graph and data analysis by Ned Mendez, Four One One.*


*Figure 28: AfD campaign poster published by an AfD politician amplifying Storm-1516 narrative. Source: CeMAS and Alliance4Europe.*[12]

[12] Translation: "Troublemakers from Ukraine are recruiting German teenagers and immigrants to commit crimes to discredit the AfD."


*Figure 29: Example of R-FBI content being amplified by AfD politician. Source: CeMAS and Alliance4Europe.*[13]


*Figure 30: Screenshot from post about prank call targeting Johann Wadephul. Source: CeMAS and Alliance4Europe.*

[13] Translation: "This must come to an end."

Stephan Protschka, a member of the German Parliament, also amplified one of the fabricated narratives promoted by Storm-1516. However the post did not gain much traction, only receiving around 430 interactions and less than 10,000 views.

The second instance was from an X account claiming to belong to AfD Hamburg-Mitte; however the official website of the party lists a different X account for this local chapter. The video (shown above) achieved significantly more reach than the average post from the account with 2.6 million views.

A separate operation saw Russian pranksters Vladimir Kuznetsov and Alexei Stolyarov call CDU MP Johann Wadephul (now Germany's foreign minister), posing as Ukrainian officials. They twisted the call to claim that CDU campaign promises would be void once the party won. Wadephul publicly addressed the prank, prompting German *media* coverage and leading to the ruse then reaching a broad domestic audience.

However the most notable case centres on an incident of vandalism which multiple German media outlets initially incorrectly blamed on radical German *climate activists*. Hundreds of cars across several German states were vandalised over the course of three days with perpetrators filling exhaust pipes with construction foam and leaving stickers promoting Robert Habeck, the Federal Minister for Economic Affairs and Climate Action and a representative of The Green Party. This story was covered by one of Germany's largest newspapers and remained uncontested for multiple days, before being confirmed via German domestic intelligence agency as being most likely *organised and directed by Russia.*

# 2025 in context of previous German elections

Considering the 2025 German federal election in the context of the two previous federal elections in 2017 and 2021, three key takeaways are important to note which provide a broader perspective on the election and valuable insights that can inform future election strategies and understanding.

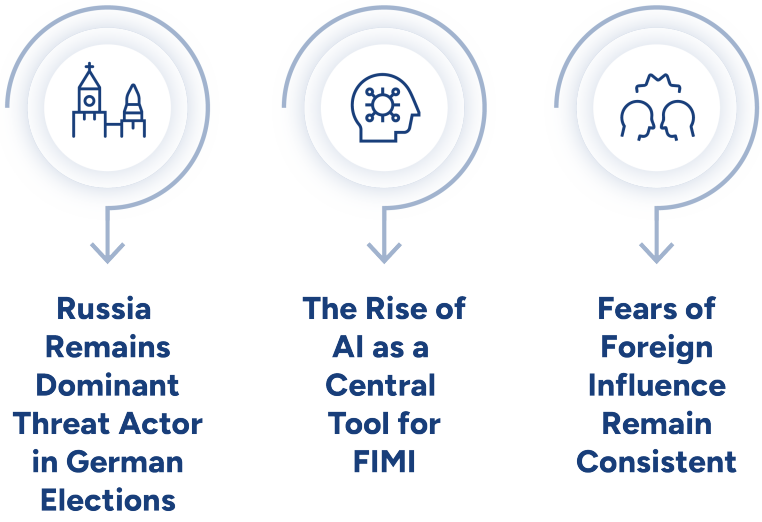



*Figure 31: 2025 in context of previous elections*

## 1. Russia remains the dominant threat actor in German elections

Russia remains the primary threat actor in German elections, at the federal as well as state level. This threat is well understood by the German population, according to *Bitkom's representative survey* of eligible voters that found nearly 90 percent believed foreign actors (primarily Russia and the US) were attempting to influence the German election through social media. Russian interference in Germany is not restricted to election periods, but its significant increase during these times is predictable and likely to escalate in the coming years.

This is especially likely should Germany maintain and increase its support for Ukraine as promised. Operations such as Doppelgänger, Overload and Storm-1516 will continue to play a large role in Germany's politics. This underscores the need for sustained vigilance and robust countermeasures to Russia's aggressive influence operations.

## 2. The rise of AI as a central tool for FIMI

The use of AI as a key tool for foreign actors to create and disseminate disinformation during German elections was identified in 2025. Deepfakes emerged as one of the most common TTPs employed by FIMI actors, especially video content. As AI technology continues to evolve and become more sophisticated, the prevalence of manipulative AI-generated content will increase and become harder to identify.

Another growing concern is that while many users may recognise content as AI-generated, they often dismiss its significance, showing little concern for its manipulative potential. This highlights the need for both strong countermeasures against AI-driven interference and broader public education and AI literacy to ensure people understand the risks and implications of engaging with synthetic media. Reinforcing these efforts is a critical investment to safeguard future elections, but also to protect the broader public from the harmful effects of AI-generated propaganda and foreign influence.

## 3. Fears of foreign influence remain consistent

As stated above, the German population has since at least 2017 worried about foreign influence in their country's elections and democratic process. The Federal Government should clearly communicate the steps it is taking to address these threats and use this widespread concern to boost media literacy and resilience among citizens. By helping people better recognise, report and resist manipulative narratives, the government can turn public awareness into a powerful tool for strengthening democracy. This genuine interest in the issue is a valuable opportunity for education and building resistance that should not be wasted.

# Interventions and responses

In response to the identified influence operations, we actively engaged in mitigation efforts across multiple levels. All instances of the Storm-1516 campaign were flagged to the respective social media platforms, including through the Digital Services Act (DSA) flagging mechanism. X declined all submitted reports of Storm-1516 activity, claiming in an email that the content is not illegal. We did not see any actions taken in any of the instances where we flagged content to X. By contrast, Bluesky implemented mitigation measures informed by our reporting. Doppelgänger drastically reduced their activities on the platform after Bluesky was informed about the pattern of behaviour of the influence operation.

Beyond platform engagement, the coalition shared findings with relevant German authorities who subsequently incorporated the material into their national threat landscape briefings. At the EU level, we coordinated with the European Commission's DSA team, the Code of Practice Secretariat and the German Digital Services Coordinator (DSC) to ensure regulatory awareness and alignment in addressing the threat. Our findings were also shared with fact-checkers and media who could inform the public about our findings, inoculating parts of the German population from their effects.

We shared our findings with the Counter Disinformation Network which has approximately 250 participating OSINT researchers, fact-checkers, journalists, academics and other practitioners as well as a wide range of German practitioners, ensuring that our findings could inform their monitoring and research.

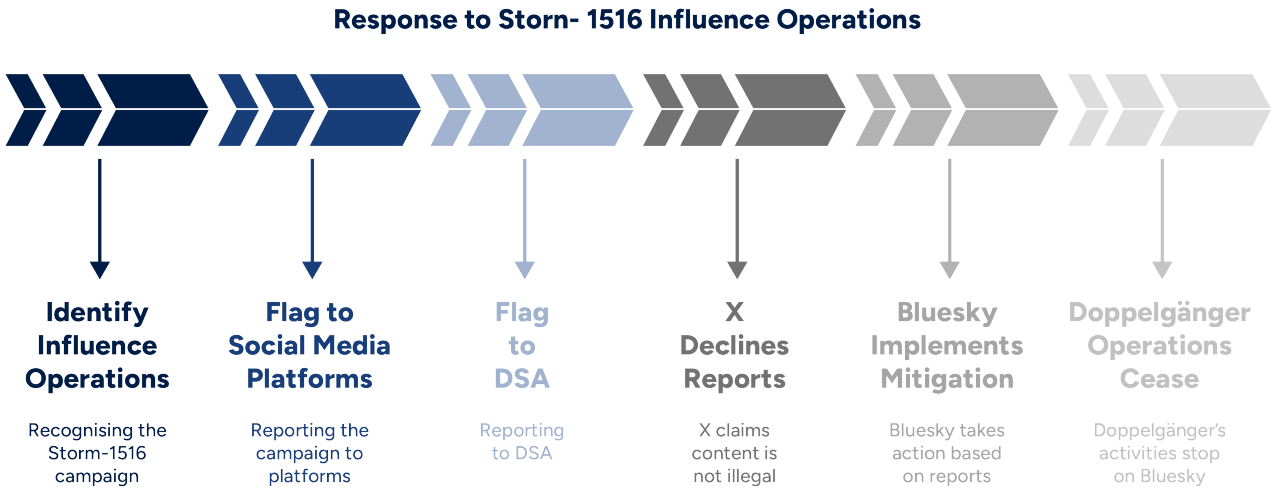



*Figure 32: Identification and response process for Storm 1516 content*

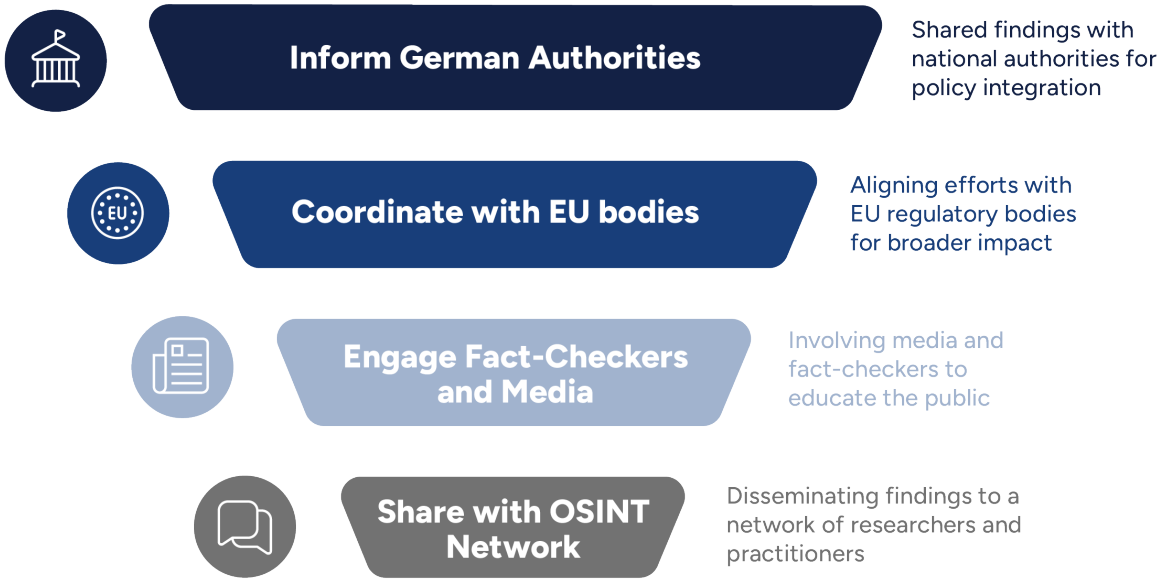



*Figure 33: Communication and coordination within the project*

# Policy recommendations

To effectively counter influence operations, we need a sustained, multi-stakeholder strategy that mobilises platforms, government, regulators and civil society in concert. OSINT researchers, fact-checkers, journalists, academics, communications specialists, security services, policy-makers and regulators all bring unique strengths and mandates. Their collaboration must extend beyond high-profile moments like elections and become a continuous, institutionalised effort.

A genuine 'whole-of-society' approach is essential for safeguarding democratic processes but it cannot succeed without dedicated resources. European governments must commit to long-term investments in democratic resilience. Specifically, the EU should leverage its Preparedness Plan to guarantee core funding for civil society organisations and establish a dedicated Democracy Shield Fund to underwrite these collective efforts. By embedding cross-sector cooperation into regular governance and ensuring steady financial backing, it is possible to build the robust, enduring defences that democracies require.

With elections increasingly targeted by foreign actors, safeguarding electoral integrity is essential to preserving democratic legitimacy. Interference efforts such as disinformation aim to distort public discourse and voter behavior. Strengthening election security through legal, technical and institutional measures will ensure that electoral outcomes will be better protected against malign influence. Democratic institutions are facing the same threats. Proactive, cross-sectoral countermeasures, including detection mechanisms, diplomatic pressure and public education, are critical to reducing their reach and effectiveness. A proactive approach helps safeguard democratic stability and public trust in political processes.

The DSA requires Very Large Online Platforms (VLOPs) to assess and mitigate systemic risks to electoral processes, including those arising from disinformation and foreign interference (Article 34 and 35). Smaller platforms (with less than 45 million average monthly active users in the EU) also have obligations regarding transparency and accountability reporting. The Bundesnetzagentur, the German Digital Services Coordinator (DSC), plays a key role in enforcing the DSA in Germany. However, proper resourcing is necessary to oversee platform compliance and support academic research. Without adequate capacity, the regulatory framework risks becoming ineffective or inconsistently applied.

Regulatory bodies, particularly in the EU and Germany, should intensify efforts to track and sanction websites distributing RT DE content. This includes monitoring alternative domains, mirror sites and traffic-redirecting platforms with sanctions applied where

Kremlin links are evident. Monetisation of such sites should be restricted with ad tech companies playing a key enforcement role. German ISPs should strengthen detection and blocking of RT mirror domains, supported by intelligence-sharing mechanisms like common blacklists. Similarly, search engines and social media platforms must improve enforcement of bans, especially where geolocation-based filtering remains *inconsistent.*

To increase transparency and limit content laundering, aggregator and podcast platforms should be encouraged to clearly label state-linked media content in line with the voluntary commitments under the Code of Practice on Disinformation. While the DSA does not mandate labelling by podcast platforms specifically, VLOPs have obligations to assess and mitigate risks related to foreign information manipulation and interference (Articles 34 and 35). Collaboration with podcast directories is needed to establish guidelines for handling material from sanctioned entities. Additionally, further investigation into the infrastructure behind RT's podcast distribution, including financial and technical enablers, is recommended.

In the digital age, transparency in political advertising is essential to protect democratic integrity. Without clear regulations, opaque advertising practices can facilitate the manipulation of voter perceptions, including through foreign-funded campaigns. Alongside the current DSA (Articles 26 and 39), the upcoming regulation (EU) 2024/900 on the transparency and targeting of political advertising addresses this by requiring online platforms to disclose the identity of sponsors and targeting criteria for political ads. Ensuring full implementation by platforms of these rules enhances electoral fairness, accountability and public trust. The European Commission and national DSCs must be supported in their role in ensuring compliance by VLOPSEs of these obligations and civil society and researchers play a vital role in providing an evidence base for such investigations.

The European Media Freedom Act (EMFA) focuses mainly on traditional media, missing the dominance of digital-native outlets, influencers and platform-based amplification. Although these companies have become de facto media organisations, the law does not subject them to the same standards of transparency and accountability as traditional news outlets. Online ecosystems have become the primary news source for many, meaning that media pluralism must include these actors. Expanding EMFA's scope would better address modern threats to editorial diversity and independence.

Effective regulation requires consistent due diligence across all actors in the information ecosystem. Media outlets and advertisers can also spread or monetise harmful content. Ensuring proper implementation of EU rules such as the DSA will enhance accountability and close loopholes that enable the spread of disinformation or manipulation. Digital disinformation campaigns often transcend national borders, requiring a unified legislative

framework and effective regional coordination. Given the complexity of cross-border challenges, regulatory efforts must still be flexible enough to accommodate national differences while fostering cooperative mechanisms.

Meanwhile, social media platforms should enhance their ability to proactively detect and disrupt CIB, particularly by preventing malicious actors from exploiting verified accounts. For instance, Bluesky is advised to apply behavioural patterns identified in our investigation to mitigate similar operations, while researchers should continue monitoring the platform for ongoing developments. Given that smaller or emerging platforms may lack the resources or incentives to act voluntarily, regulatory frameworks should incentivise or require compliance with these standards to ensure consistency across the ecosystem.

With regard to election-specific disinformation, regulators should be alerted to initiate further action. Targeted media outlets and institutions should be informed to raise awareness and build resilience. To counter spoofing and impersonation efforts, we recommend archiving relevant accounts and content to support future research, refining surfacing techniques and flagging these accounts for removal. Finally, public awareness campaigns should highlight the tactics of operations such as Storm-1516 to prevent unintentional amplification and strengthen democratic safeguards.







***Amman | Berlin | London | Paris | Washington DC***



*www.isdglobal.org*

FIMI RESPONSE TEAM REPORT

# FOREIGN INFORMATION MANIPULATION AND INTERFERENCE (FIMI) - INFORMATION SHARING AND ANALYSIS CENTRE (ISAC)