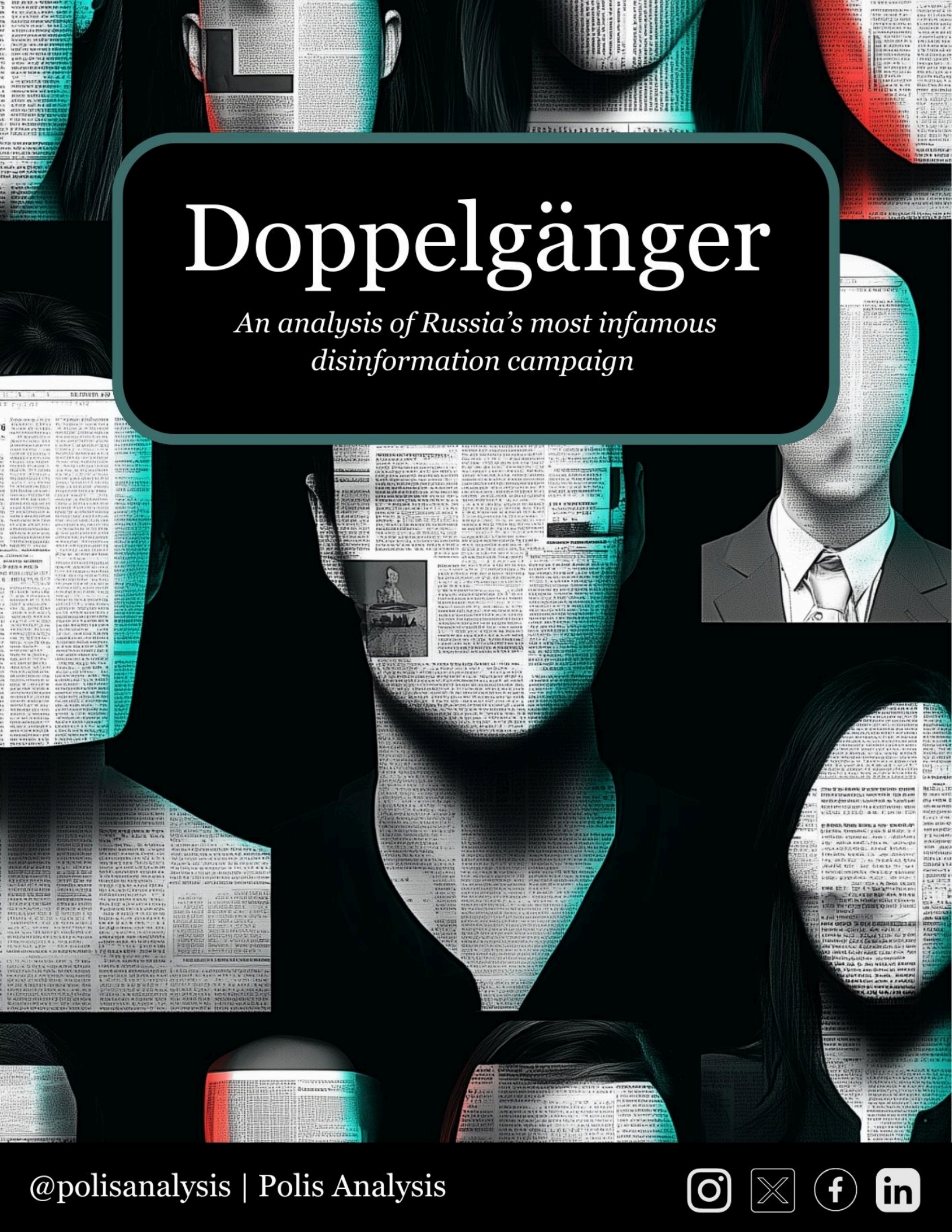


# Doppelgänger

*An analysis of Russia's most infamous disinformation campaign*

@polisanalysis | Polis Analysis

# About Polis Analysis

Polis Analysis is a provider of high-quality analysis of global politics with teams based in the heart of political capitals including London, Brussels, Berlin, Paris, Istanbul, Washington D.C., and New Delhi. Our next-generation team of experts bring a fresh and innovative approach to political analysis, which is delivered in an impartial, fact-based, and accessible way.

The political media space is a crowded field. However, media coverage of international politics is increasingly polarised and partisan in recounting stories. Even those consultancies that provide rigorous analysis instead of sensationalist media coverage deliver it to the exclusive preserve of big corporations and wealthy clients. At Polis Analysis, we do things differently. Our next-generation team is uniquely placed to deliver a new way of covering global politics. We don't simply recount political stories; we analyse them to explain their significance to your life.

# Acknowledgements

The Polis Analysis team would like to extend their appreciation to the dedicated individuals whose collective efforts have made the publication of this briefing possible. We would like to thank Founder and CEO Thomas Barton and our Advisory Board who have made this endeavour possible.

We express our sincere gratitude to members of the Digital Media Observatory, namely Khuslen Ganzorig, Raphaël Péchère-Burns, Grace Mills, and Joseph Atkinson for their excellent contributions to this text, as well as Digital Media Observatory lead Joshua Tyler for editorial overview and publication.

## Table of Contents

# Introduction

Doppelgänger is a Russia-linked malign foreign influence campaign.[1] [2] Campaigns primarily consist of thousands of fake social media accounts on various social media platforms such as Facebook, Instagram, YouTube, X, and Telegram. These accounts are used to spread false content published on copy websites, establishing a complex web of false information. These websites share identical design and branding intertwined with fabricated narratives propagating pro-Kremlin disinformation.

Topics of choice often concern the war in Ukraine, perceived economic hardship for the West due to sanctions, or alleged governmental corruption. Content is often localised, translated to specific languages and cultural contexts to reinforce pre-existing societal divisions, while paid promotions on platforms such as Facebook have previously taken place.

The central goal of Doppelgänger is believed to be to undermine support for Ukraine, further incite Western political and social divisions, and erode trust in Western media and public institutions. Notwithstanding ongoing disruptions by platform providers and cybersecurity entities, "Doppelgänger" has demonstrated a persistent threat to information integrity in the West, adapting its techniques and infrastructure to evade detection while showing a continued and methodical effort to influence opinion.[3]

Doppelgänger is primarily linked to Russian groups and individuals who have been sanctioned by the US Department of Justice for taking part in foreign malign foreign influence operations, with the influence campaign directly being tied to the Russian state through First Deputy Chief of Staff of the Presidential Executive Office Sergei Vladilenovich Kiriyenko.[4]

---

[1] https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/
[2] https://www.disinfo.eu/doppelganger-operation
[3] https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf
[4] https://home.treasury.gov/news/press-releases/jy2559

# Timeline

**March 2022:** Domain RRN (Russian Reliable News) created and registered in Russia, fronting as an independent news outlet that provides fact-checked news. Articles are identical to those previously published on a known fake Russian fact-checking website *War on Fakes*, created immediately after Russia's invasion of Ukraine.[5]

**May 2022**: The Doppelgänger campaign is accredited by US Cyber Command to at least have been operating by this month. Acts included cloning and mimicking trusted Western media outlets to spread pro-Kremlin/ anti-Ukraine propaganda using inauthentic facebook pages.[6]

**September 2022:** Doppelgänger is publicly exposed by EU DisinfoLab. Through domain monitoring, uncovering burner accounts, leveraging internet data, investigation found over 50 domains cloning 17 legitimate and trusted media outlets (The Guardian, Bild, RBC Ukraine, Ansa…) with content designed for many European populations (UK, France, Germany, Italy, Latvia, Lithuania, Estonia). Resulted in a coordinated takedown of over 2000 social media accounts and pages.[7] [8]

**December 2022:** Meta's internal investigation identifies RRN to be part of the wider Doppelgänger's campaign and traces the beginnings to two Russian companies: *Strucura National Technologies* and *Social Design Agency*. Also uncovered a shift in Doppelgänger's tactics, with less emphasis on publishing fabricated news outlets and more emphasis on social media bots to drive influence.[9]

**June 2023:** France officially accuses Russia of an orchestrated disinformation campaign and issues the first governmental condemnation. VIRGINUM identifies over 50 fake articles and more than 300 domains mimicking French governmental sites (Ministry of Europe and Foreign Affairs) and media outlets (Le Monde, Le Parisien, 20 minutes) spreading disinformation surrounding Western sanctions against Russia, fake tax policies, refugee propaganda and fabricated stories surrounding Ukraine.[10] [11] [12]

Microsoft reports that Storm-1679 (a Doppelgänger operator) has released "Olympics has fallen," a feature length film depicting AI generated Tom Cruise criticising the International Olympics Committee

---

[5] https://www.sgdsn.gouv.fr/files/files/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN1.pdf
[6] https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/
[7] https://www.sgdsn.gouv.fr/files/files/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN1.pdf
[8] https://www.disinfo.eu/doppelganger-operation
[9] https://euvsdisinfo.eu/uploads/2024/06/EEAS-TechnicalReport-DoppelgangerEE24_June2024.pdf?utm_source=chatgpt.com
[10] https://www.disinfo.eu/disinfo-update-13062023/?utm_source=chatgpt.com
[11] https://apnews.com/article/france-russia-disinformation-ukraine-war-1cbd631f2abdde39311eec52005043be?
[12] https://euvsdisinfo.eu/uploads/2024/06/EEAS-TechnicalReport-DoppelgangerEE24_June2024.pdf?utm_source=chatgpt.com

and amplifying concerns of safety in Paris/ terror threats, spread in the build up to the Paris Olympics 2024.[13]

**July 2023:** Germany accuses Doppelgänger of cloning major German news sites (Die Welt, De Spiegel, FAZ…) and used over 50,000 X bots to promote and amplify the fake websites.[14]

**August 2023:** Doppelgänger expands to targeting both French and US media including Fox News, The Washington Post, and Liberation, spreading disinformation surrounding the Russia-Ukraine war. Meta describes this as the "largest and most aggressive persistent covert influence operation from Russia."[15]

**October-December 2023:** False anti-Ukraine stories circulating Estonia. VIGINUM and Estonian Foreign Intelligence Service attribute sentiments that Ukrainian refugees are displacing Estonian citizens to Doppelgänger.[16]

**December 2023:** Further amplification of use of AI- generated content to distribute fake news and exacerbate tension. French officials accuse Doppelgänger and RRN of being the first site to spread Star of David Grafitti in Paris.[17]

Doppelgänger-linked sites spread false celebrity endorsements of pro-Russian and anti-Ukrainian sentiments using fake quotes and false social media posts, impersonating celebrities like Taylor Swift, Emma Watson and Arnold Schwarznegger.[18]

**January- February 2024:** Politico reports that over 100 new domains mimicking German news sites are created, with over 50,000 new fake X accounts posting upwards of 3000 tweets per day, all promoting fake stories, deepfakes and AI manipulated videos favoring the Alternative für Deutschland (AfD) and discrediting pro-Ukrainian politicians.[19]

**March 2024:** False images of Estonian ministers mocking Russian speaking citizens going viral on social media.[20]

---

[13] https://blogs.microsoft.com/on-the-issues/2024/06/02/russia-cyber-bots-disinformation-2024-paris-olympics/
[14] https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/kremlin-info-ops-in-europe-and-the-caucasus/?utm_source=chatgpt.com
[15] https://www.foxnews.com/world/china-russia-behind-largest-cross-platform-misinformation-operation-meta-report-finds?
[16] https://www.ifes.org/pub/building-resilience-against-election-influence-operations-/case-studies
[17] https://www.euronews.com/my-europe/2023/11/23/doppelganger-how-a-russian-disinformation-campaign-is-exploiting-the-israel-hamas-war?
[18] https://www.wired.com/story/russia-ukraine-taylor-swift-disinformation/?utm_source=chatgpt.com
[19] https://www.politico.eu/article/germany-election-flood-social-media-x-russia-bots-kremlin-operation-false-news/
[20] https://en.respublica.lt/disinformation-actors-focus-on-topics-ranging-from-the-events-of-the-russia-ukraine-war-to-refugees?

**May 2024:** Open AI confirms removing multiple accounts linked to Doppelgänger operations that were used to create headlines and content for spoof websites and generate social media comments in multiple European languages (English, French, German, Italian and Polish). Misinformation on EU migration policies and AI-generated content of fake riots supposedly caused by Ukrainian migrants spread around Lithuania, Latvia and Estonia with sentiments exacerbated on spoof news sites with AI generated comments.[21] [22]

**June 2024:** European nations affected by Doppelgänger during the 2024 EU elections. Meta, VIGINUM, CeMAS, ISD, Hybrid Warfare Analytical Group and various governmental agencies in France, Germany and Poland all allege Doppelgänger interference in election campaigns. Articles presenting negatives surrounding Ukrainian Aid were spread around Italy and Spain, anti-NATO sentiments were spreading throughout Slovakia, Czechia and Poland. Far-right amplification, false reports on Gaza, and smear campaigns were present throughout France and Germany.[23] [24]

**September 2024:** Experts in the US seize over 30 Kremlin and Doppelgänger-linked domains Spoofing US media outlets including Fox News and The Washington Post, accusing Doppelgänger of paying influencers and using AI-generated content to attempt to influence the 2024 Presidential Election. Yet DFRLab claims that multiple new Doppelgänger-linked domains were immediately created within hours of the initial group of 30+ being seized.[25]

**October 2024:** The UK_sanctions three Russian agencies (SDA, Structura, ANO DIALOG) and three senior figures (Ilya Andreevich GAMBASHIDZE, the founder of SDA, Nikolay Aleksandrovich TUPIKIN, the CEO of SDA and owner of Structura, Andrey Naumovich PERLA, SDA Project Director).[26]

**April 2025:** Poland detects Doppelgänger interference through the Polish Presidential Campaign with over 250 X posts spreading NATO conspiracies and anti-migrant sentiments. NATO reports SDA campaigns targeting Estonia, Latvia and Lithuania spreading conspiracy theories and false migration riots. The CEO of a company alleged to host servers tied to Doppelgänger, Yuri Bozoyan, is arrested in Russia on suspicion of leading a criminal organization and involvement in large-scale drug trafficking.

---

[21] https://downloads.ctfassets.net/kftzwdyauwt9/5IMxzTmUclSOAcWUXbkVrK/3cfab518e6b10789ab8843bcca18b633/Threat_Intel_Report.pdf

[22] https://en.respublica.lt/disinformation-actors-focus-on-topics-ranging-from-the-events-of-the-russia-ukraine-war-to-refugees?

[23] https://euvsdisinfo.eu/uploads/2024/06/EEAS-TechnicalReport-DoppelgangerEE24_June2024.pdf

[24] https://www.reuters.com/world/europe/european-election-how-eu-says-russia-is-spreading-disinformation-2024-06-03/?

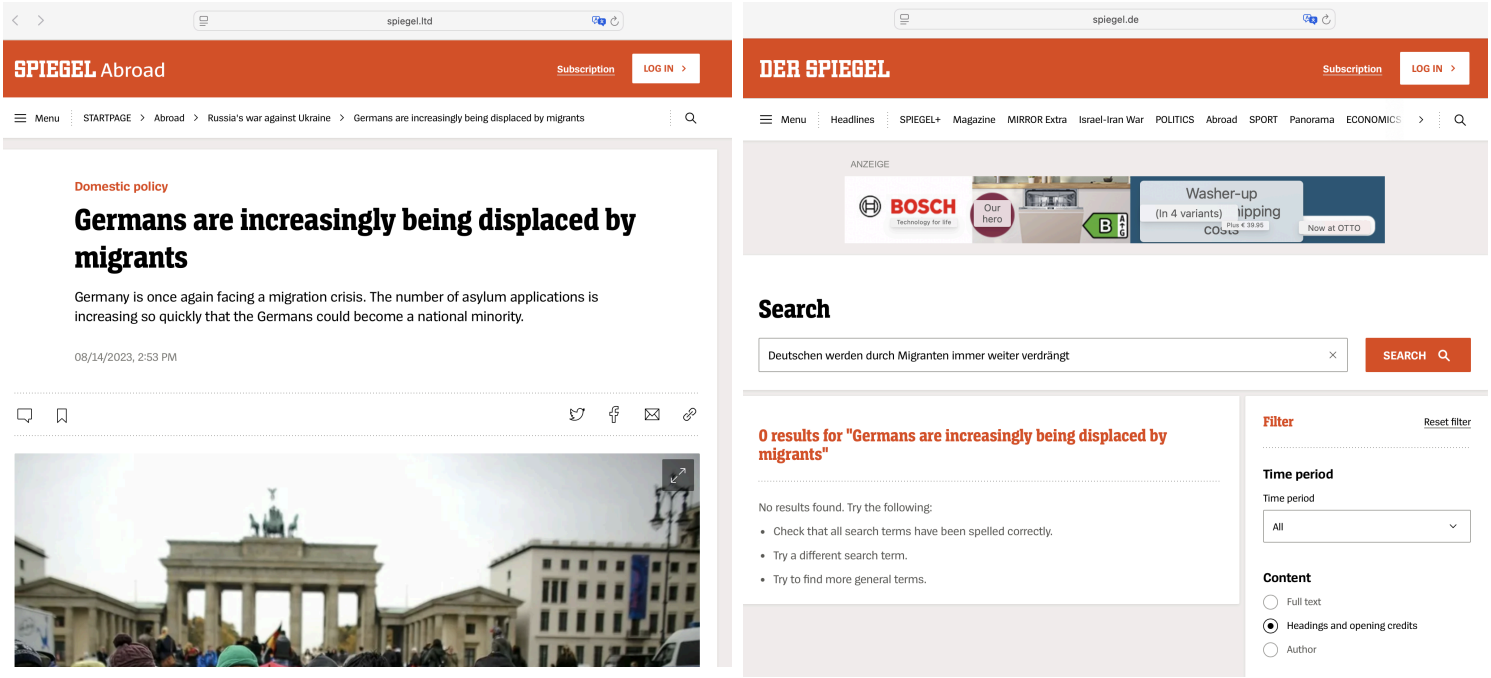
[25] https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

[26] https://www.gov.uk/government/news/uk-sanctions-putins-interference-actors

# Case Study: Spiegel.ltd

The replication of Der Spiegel's website is a clear example of how the reputation of credible news outlets can be exploited to spread disinformation. Although many news organisations including Le Monde, The Guardian, and Fox News have been targeted by the Doppelgänger operation, German news outlet Der Spiegel provides a unique insight as its copy remains live at the time of this report.

The official domain of Der Spiegel is spiegel.de, while its Doppelgänger counterpart sits under spiegel.ltd. On WHOIS, a public database storing registration data for domain names, spiegel.ltd was registered 29 June 2022, four months after the Russian invasion of Ukraine.[27] Spiegel.ltd does not operate as a standalone website, and if you attempt to search spiegel.ltd you will be redirected to the official Der Spiegel site. Doppelgänger relies on fake social media accounts to post links to the actual fake articles and videos on the mirror site, and bots disseminate the link with other users through the comment section of platforms such as Facebook.[28]




*Doppelgänger website spiegel.ltd (Left) containing an article titled "Germans are increasingly being displaced by migrants, which cannot be found on Der Spiegel's legitimate website, spiegel.de (right).*

As seen above, one link for example will take you to a German-language "domestic policy" article on spiegel.ltd with the headline 'Deutschen werden durch Migranten immer weiter verdrängt' ("Germans

[27] https://whois.domaintools.com/spiegel.ltd

[28] https://mpf.se/psychological-defence-agency/publications/archive/2025-05-15-beyond-operation-doppelganger-a-capability-assessment-of-the-social-design-agency

are increasingly being displaced by migrants").[29] The article mimics the investigative journalistic style of Der Spiegel. It has cited legitimate figures from the Federal Office for Migration and Refugees, the European Conservative, Dow Jones, and Die Welt. This article ultimately, and subtly, creates the impression that Der Spiegel is in support of the AfD and is against the wave of Ukrainian and Muslim refugees. If the reader tries to navigate this webpage, the website is smoothly redirected to the official spiegel.de.

A French cybersecurity company, HarfangLab, examined the disinformation chain, exploring how social media accounts are responsible for posting the links that redirect users to Doppelgänger's site.[30] According to HardangLab, while final content URLs were mostly Doppelgänger sites, some also went to completely fabricated news outlets or legitimate sites belonging to organisations that already promote pro-Kremlin content, such as stratpol.com and liberationnews.org. This demonstrates the broader Russian strategy of utilising the reputation of diverse media sources to push pro-Kremlin propaganda into mainstream spaces.

[29] https://www.spiegel.ltd/ausland/Deutschen-werden-durch-Migranten-immer-weiter-verdr%C3%A4ngt-a-61180844-af5d-4fb9-993e-a245ea38053d.html

[30] https://harfanglab.io/insidethelab/doppelganger-operations-europe-us/

# Analysis

## Intelligence Aims:

Doppelgänger's intelligence priorities centre on short-term strategic disruption rather than long-term ideological influence, with three interlinked objectives: (1) undermining Western support for Ukraine, (2) exacerbating political and social divisions within target states, and (3) eroding trust in Western media and public institutions.[31]

To achieve this, Doppelgänger engages in epistemic subversion, deploying cloned media outlets and mimicking trusted visual branding to blur the line between fact and fiction.[32] By planting credible-seeming falsehoods, it corrodes trust and fosters cynicism without triggering immediate suspicion or attribution. This tactic is especially potent during elections, when public confidence is fragile, where rather than advocating positions, Doppelgänger utilises polarising issues: immigration, LGBTQ+ rights, vaccine mandates, and economic inequality, to inflame divisions and weaken social cohesion.[33] [34]

Furthermore, Doppelgänger also targets emerging events, filling information spaces before detection systems can respond. Its use of AI-generated content and disposable dissemination infrastructure enables scalable campaigns that align and respond to audience biases, outpacing and overwhelming moderation systems.[35] Crucially, the primary intelligence objective is not to persuade audiences of a new reality, but to dismantle their trust in the one they already have.

## Comparison to Iranian, Chinese Influence Campaigns:

While Doppelgänger's campaigns share tactics with other state-linked influence operations, such as China's United Front Work Department and Iran's International Union of Virtual Media, their effectiveness stems from focused intelligence objectives and advanced dissemination systems.[36] [37] Doppelgänger represents a more sophisticated evolution of state-linked disinformation, distinct from the declarative ideological framing common to Iranian operations and the long-term narrative engineering characteristic of Chinese influence efforts.[38] [39] While it shares a degree of subtlety with China,

---

[31] https://www.disinfo.eu/doppelganger-operation/
[32] https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/
[33] https://www.psychologicaldefence.lu.se/sites/psychologicaldefence.lu.se/files/2025-05/Beyond%20Operation%20Doppelgänger.pdf
[34] https://www.intrinsec.com/doppelganger-new-disinformation-campaigns-spreading-on-social-media-through-russian-networks/
[35] https://www.recordedfuture.com/research/russian-influence-network-doppelgangers-ai-content-tactics
[36] https://www.bbc.co.uk/news/articles/c878evdp758o
[37] https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://home.treasury.gov/news/press-releases/sm1158&ved=2ahUKEwj7gOuYv6WOAxV4WUEAHUFLJrYQFnoECBgQAQ&usg=AOvVaw3UkzGGflb_R_BBwB8x-u2L
[38] https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/
[39] https://www.aspi.org.au/report/truth-and-reality-chinese-characteristics/

Doppelgänger differs markedly in method and intent, prioritising tactical speed, fragmentation, and disruption over coherence or persuasion.

In this sense, Doppelgänger campaigns resemble information insurgency or guerrilla warfare: deploying AI-generated content through cloned media outlets, amplifying it via bot networks, disappearing before detection systems can respond, and later resurfacing in altered forms.[40] [41] This model enables Doppelgänger to exploit high-impact events with locally tailored, credible disinformation, saturating platforms with disinformation that is difficult to trace, moderate, or attribute in real-time.

Thus, in contrast to both Chinese and Iranian models, Doppelgänger focuses less on constructing stable counter-narratives. Instead, it seeks to exhaust the very notion of truth, with its structure and methods making it not only harder to effectively moderate but more corrosive in its intent than both Chinese and Iranian efforts.[42] By abandoning ideological coherence, it challenges conventional models of propaganda analysis and redefines influence as disruption, rather than persuasion, enabled by emerging technologies such as AI.

## AI Automated Systems:

Central to the effectiveness of its campaigns is the leveraging of AI-generated content and automated bot-based dissemination networks to scale and adapt its operations. Generative AI is used to create high volumes of tailored, persuasive articles and deepfake imagery that mimics the tone and structure of legitimate sources and journalism.[43] This content is then distributed through a two-tiered system of bots: 'originator' bots generate the initial posts, often linking to cloned media outlets, while 'amplifier' bots repost this content as replies to trending topics or high-profile accounts.[44] Combined, this two-tiered system creates the illusion of organic engagement.[45]

Additionally, to decrease traceability, many of these bot networks are deliberately disposable – designed for short-term use and quickly replaced. This strategy helps prevent the buildup of a persistent signature, making attribution more difficult and reducing the risk of detection by moderation systems.[46] Unlike earlier influence operations that relied on human coordination, Doppelgänger's integration of AI-generated content and scalable bot networks enables a disinformation model that is fast-moving, deniable, and constantly evolving, making it significantly more challenging to counter or contain in real-time.

---

[40] https://www.polytechnique-insights.com/en/braincamps/geopolitics/asymmetrical-warfare-new-strategies-on-the-battlefield/guerrilla-2-0-asymmetric-warfare-in-the-tech-era/

[41] https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/

[42] https://arxiv.org/abs/2505.07212

[43] https://www.doppel.com/blog/russian-disinformation-campaign-doppelganger-is-why-doppel-exists

[44] https://dfrlab.org/2024/09/06/how-doppelganger-and-other-russia-linked-operations-target-us-elections/

[45] https://medium.com/dfrlab/from-russia-with-hategroup-ae6ee4318b5b

[46] https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

## Geofencing:

Doppelgänger also utilises location-based targeting to enhance the precision and effectiveness of its campaigns. It deploys geofencing, using GPS and IP data to create virtual geographic boundaries, enabling locally-tailored disinformation that remains hidden from external observers and researchers.[47] For example, access to a fake Fox News site may be exclusively accessible to US-based IP addresses, while all other users are redirected to a blank page.[48] This approach tailors content to local contexts, ensuring high engagement, minimising detection by unintended actors, and reinforcing deniability of its operations.[49]

---

47 https://www.hivepro.com/wp-content/uploads/2024/02/Unmasking-Doppelganger-Russias-Disinformation-Campaign-Revealed_TA2024078.pdf

48 https://www.nbcnews.com/tech/misinformation/-kremlin-x-accounts-push-fake-fox-news-articles-ahead-debate-rcna159301

49

*Navigate the Political World.*

@polisanalysis | Polis Analysis