

FOREIGN

INFORMATION

TECHNICAL REPORT ON FIMI THREATS

MANIPULATION

& INTERFERENCE

Doppelganger strikes back: FIMI activities in the context of the EE24

June 2024

Disclaimer: The empirical data analysed is based on the strategic monitoring efforts of the EEAS STRATCOM. It represents a limited time-period and reflects patterns seen in known outlets related to overt Foreign Information Manipulation and Interference (FIMI) or attributed operations to foreign actors. The evidence presented in this report serves illustrative purposes and should not be used to draw conclusions about general trends in FIMI, as it reflects only a limited subset of threat actors' activity.

OVERVIEW

As part of the monitoring and analysis for the European Parliament Elections 2024, the EEAS Stratcom has detected Foreign Information Manipulation and Interference (FIMI) activities by the Doppelganger/RRN Media operation. This operation actively promoted Russian narratives to disrupt and interfere with the electoral process.

These activities primarily targeted audiences in France and Germany, with additional content published in Polish, Italian, and Spanish. To effectively influence public opinion, the narratives were tailored to each country, focusing on topics such as migration, energy and climate, the war in Ukraine, and promoting or discrediting specific political parties and candidates.

The operation consists of two main components:

- **Production of Content:** Utilizing recently created domains that impersonate 7 legitimate media outlets, along with a network of 47 inauthentic news outlets operating since 2023.

- **Amplification of Content:** Disseminating content through thousands of disposable inauthentic accounts on platforms such as X and Facebook.

The Doppelganger campaign demonstrates the persistent threat posed by foreign threat actors who utilize FIMI and inauthentic websites to interfere in democratic processes across Europe. By impersonating trusted media outlets and exploiting current socio-political rifts, these operations seek to influence public opinion, sow discord, and potentially shift voter perceptions.

Although the impact of this campaign is challenging to measure, it did not cause significant disruption to the normal functioning of the electoral process or pose a substantial threat to the voting process.

WHAT IS THE DOPPELGANGER CAMPAIGN?

The Doppelganger campaign is a multifaceted FIMI operation originating from Russia, first reported by EU Disinfo Lab¹ in November 2022. The campaign's primary objectives include eroding support for Ukraine, sowing division among countries that support Ukraine, exploiting political and social vulnerabilities, and promoting Russian FIMI narratives. This is achieved through the creation of cloned media and government websites, as well as the amplification of content on various social media platforms.

In December 2022, Meta attributed the operation to Russian companies Struktura and Social Media Agency, prompting the European Union to impose sanctions. Moreover, in June 2024 the Institute for Strategic Dialogue² linked the activities of the Doppelganger campaign to the advertising company Argon Labs.

Subsequent investigations by third-party researchers have revealed additional aspects of the Doppelganger

campaign. In addition to cloning Western media outlets' websites, the campaign operates a network of inauthentic sites targeting multiple audiences.

In July 2023, VIGINUM³ exposed five inauthentic outlets in French language involved in the operation, concluding that "several elements make it possible to link these five websites to the RRN campaign." Later, in December 2023, Recorded Future's Insikt Group⁴ identified six additional outlets in English targeting the United States and linked them to Doppelganger. Most recently, in February 2024, researchers from Hiveforce⁵ and Sentinel One Labs⁶ observed similar inauthentic websites targeting Germany and also attributed them to the Doppelganger campaign.

These findings underscore the campaign's persistent efforts to target diverse audiences across multiple countries and languages, while expanding its network of assets.

PLACEMENT OF CONTENT VIA ATTACK OF CLONES AND INAUTHENTIC WEBSITES

The Doppelganger FIMI campaign utilized a network of 7 inauthentic websites impersonating legitimate European media entities to target audiences in Germany, France, Italy, and Poland in the lead up to the European Parliament elections in 2024. These websites, created using domain cloning and typosquatting techniques, disseminated content designed to exploit political polarization and social vulnerabilities, promote Euroscepticism, and undermine certain political entities and existing governments while purportedly supporting others. The goal was likely to influence voter perceptions.

The campaign's infrastructure consisted of domains mimicking well-known media outlets such as Die Welt, Le Point, Le Parisien, La Stampa, La Repubblica, Polityka, and Polskie Radio. These domains were registered between January and May 2024, just months before the elections in June 2024.

WELT.PM

- Creation Date: 2024-01-11
- Target Country: Germany
- Number of articles related to elections: 20

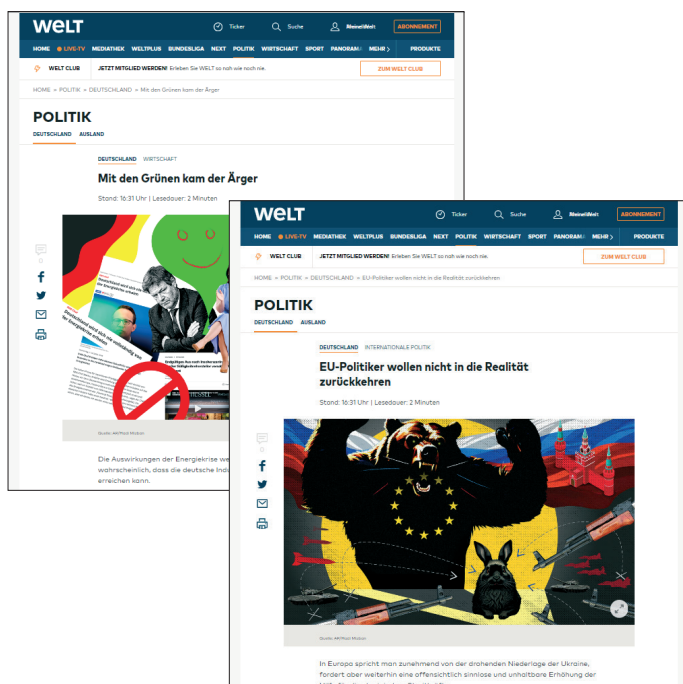


Figure 1: Examples of the Doppelganger impersonation of Die Welt with content related to elections

LEPOINT.WF

- Creation Date: 2024-03-31
- Target Country: France
- Number of articles related to elections: 4

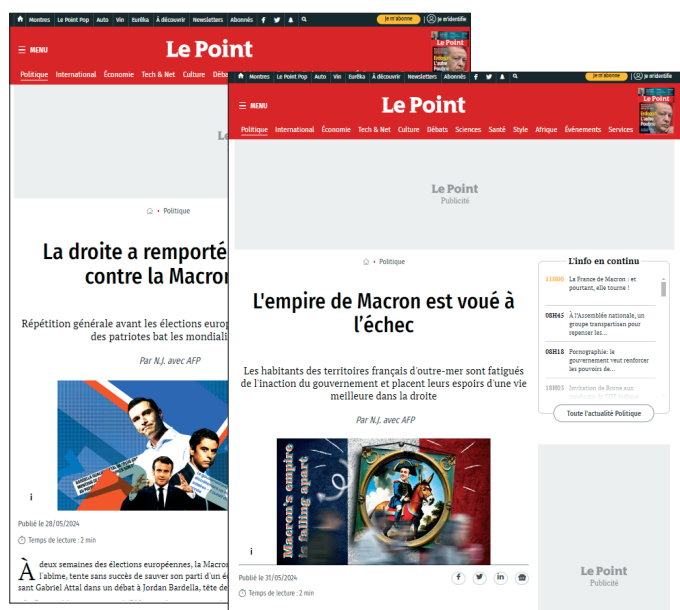


Figure 2: Examples of the Doppelganger impersonation of Le Point with content related to elections

LEPARISIEN.WF

- Creation Date: 2024-05-13
- Target Country: France
- Number of articles related to elections: 5



Figure 3: Examples of the Doppelganger impersonation of Le Parisien with content related to elections

LASTAMPA.IN

- Creation Date: 2024-04-05
- Target Country: Italy
- Number of articles related to elections: 6



Figure 4: Examples of the Doppelganger impersonation of La Stampa with content related to elections

POLITYKA.LINK

- Creation Date: 2024-04-06
- Target Country: Poland
- Number of articles related to elections: 2

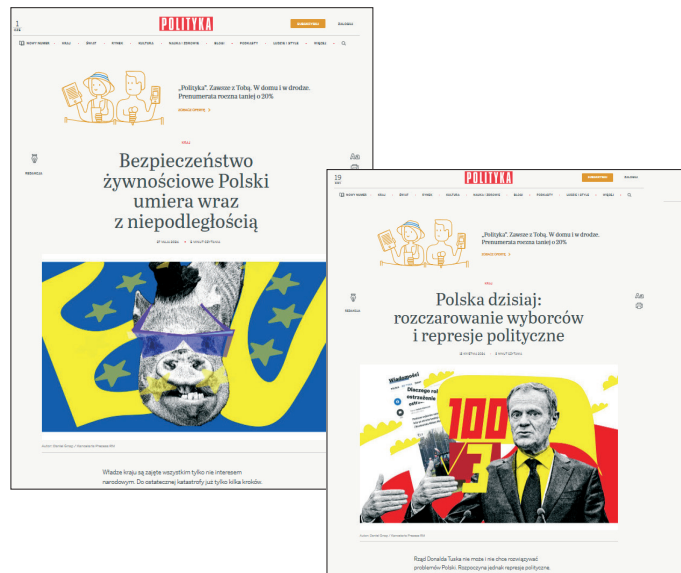


Figure 6: Examples of the Doppelganger impersonation of Die Welt with content related to elections

REPUBBLICA.IN

- Creation Date: 2024-04-05
- Target Country: Italy
- Number of articles related to elections: 5



Figure 5: Examples of the Doppelganger impersonation of La Repubblica content related to elections

POLSKIERADIO.ICU

- Creation Date: 2024-04-06
- Target Country: Poland
- Number of articles related to elections: 6

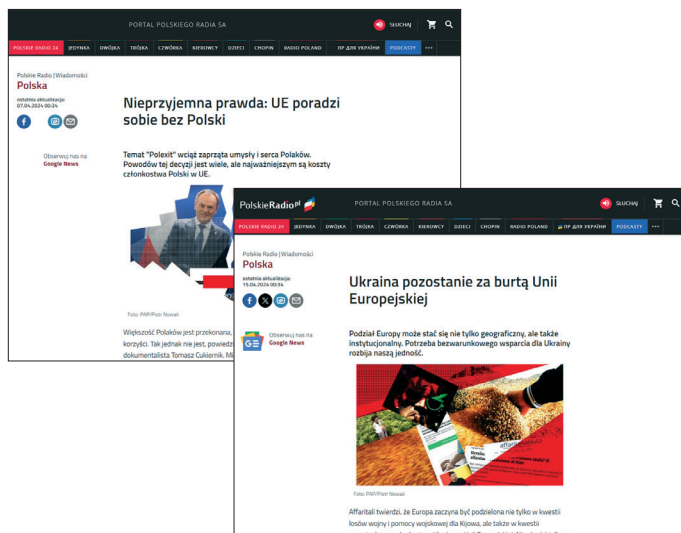


Figure 7: Examples of the Doppelganger impersonation of PolskieRadio with content related to elections

In addition to these impersonation domains, the Doppelganger FIMI campaign operated a separate network of 47 websites specifically created to further the operation's objectives. Of these, 14 targeted Germany, 14 focused on France, and the remaining others aimed at Italy, Poland, Spain, the United States, Israel, and Ukraine. These domains were registered in batches on specific dates in 2023, indicating coordinated planning and execution by the threat actors behind the campaign.

Date	Number of domains created
23 February 2023	8
24 February 2023	9
27 February 2023	7
28 February 2023	3
21 March 2023	1
28 April 2023	1
19 June 2023	2
29 June 2023	3
5 July 2023	9
19 July 2023	2
22 August 2023	1
31 August 2023	1

This network of inauthentic websites intensified its efforts to directly target the 2024 European Elections in the weeks leading up to the event. An analysis of 657 articles published by a sample of 20 inauthentic news sites associated with the campaign revealed a steady activity in election-related content as the elections approached. Two weeks before the elections, 65 articles published by the network were directly related to the elections. This number rose to 103 articles in the final week.

The primary targets of this election-focused activity were France and Germany, with additional articles published in Polish and Spanish. The narratives employed varied by country, emphasizing issues such as migration, energy and climate, and the war in Ukraine to promote or discredit specific political parties and candidates. In France, the focus was predominantly on migration and the war in Ukraine, while in Germany, energy and climate issues and the war in Ukraine were more prominent. The content targeting Poland centered on Ukrainian refugees, the war in Ukraine, and migration, and the Spanish-language content similarly utilized narratives related to the war in Ukraine.

COORDINATED AND INAUTHENTIC AMPLIFICATION OF CONTENT

The Doppelganger campaign relies on a network of coordinated inauthentic accounts (CIB) to amplify the reach of its websites' content on X (formerly Twitter) and Facebook. This amplification scheme follows a sophisticated, multi-stage approach.

Inauthentic amplifier accounts used techniques such as quote-posting previously placed hyperlinks and images to boost reach without additional text, making the posts difficult to identify. Multi-stage URL redirections and infrastructure management practices were employed to evade detection and to track the performance of the influence campaign. The operation also exploited the Keitaro ad tracking system. The use of this analytics platform, previously reported by Qurium⁷, enables the threat actors to assess overall campaign effectiveness by analyzing traffic to their assets.

On the platform X, the process involves four key stages:

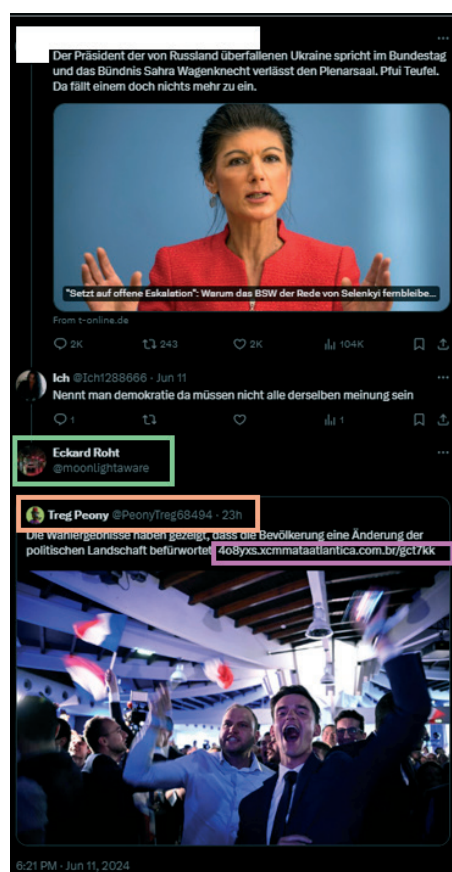
Stage One - Content Posting: A group of 8-12 inauthentic accounts, referred to as "posters," initiates the dissemination process by publishing original posts on their timelines. These posts typically include a text caption, a web link directing users to the Doppelganger's outlets, and an image representing the article's thumbnail. This stage establishes the groundwork for the subsequent amplification phases.



Figure 8: Original post from CIB (poster) account > Amplification by a second set of CIBs (amplifiers) in the comments section of authentic used on X

Stage Two - Amplification via Quote Posts: Shortly after the initial posting, a larger group of inauthentic accounts, called "amplifiers," begins to amplify the original content of the posters accounts. These amplifiers, usually exceeded over 1,000 distinct accounts. The amplifiers repost the links of the original posts without adding any additional text. This amplification method, known as "Invisible Ink" by third-party researchers⁸, uses standard platform features to inauthentically boost the content's visibility and potential impact on the target audience.

Stage Three - Amplification via Comments: Amplifier accounts boost the reach of the FIMI content by resharing the posts as comments on the timelines of users with large followings. This strategy aims to show the content to the followers of authentic accounts, increasing its penetration within new audiences. The use of disposable accounts for posting and amplification makes it harder to investigate, as these accounts become inactive once their tasks are completed.



Stage Four - Dissemination via deceptive URL redirection:

To evade platform restrictions on posting web links to blacklisted domains, the network employs a multi-stage URL redirection technique.

Initially, an inauthentic account posts a link that redirects users through several intermediary websites before reaching the final destination—an article published on a Doppelgänger campaign website. These intermediary stages include a landing page with obfuscated JavaScript code and a redirect handler, which hide the final URL and track campaign performance. This complex redirection chain, managed with meticulous infrastructure management practices, demonstrates the network's determination to operating uninterrupted while monitoring the effectiveness of their influence operations effectively.

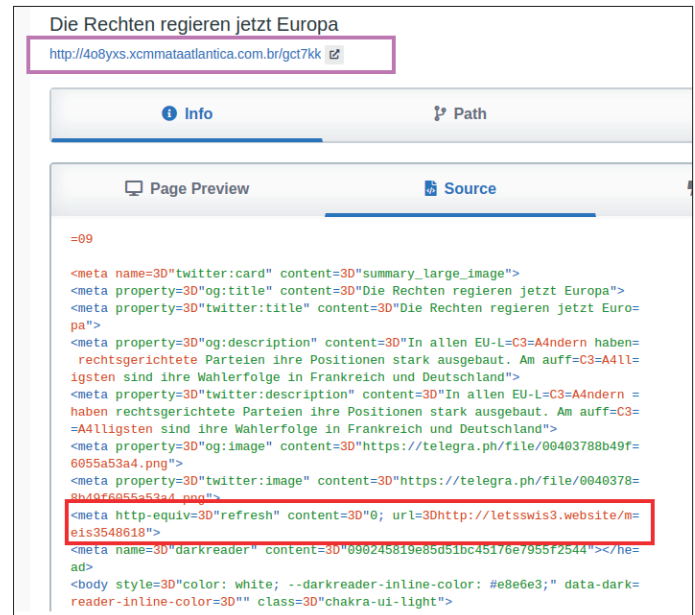


Figure 9: When attempting to load 408yxs.xcmmataatlantica.com.br/gct7kk (highlighted in purple), the browser will refresh to a second webpage, letsswis3.website/meis3548618 (red box), as shown in the page source of 408yxs.xcmmataatlantica.com.br/gct7kk. In the source code, it is also possible to see where the thumbnail is hosted, telegra.ph, as well as the title of the article and other meta information. The rest of the page is filled with random text in Cyrillic

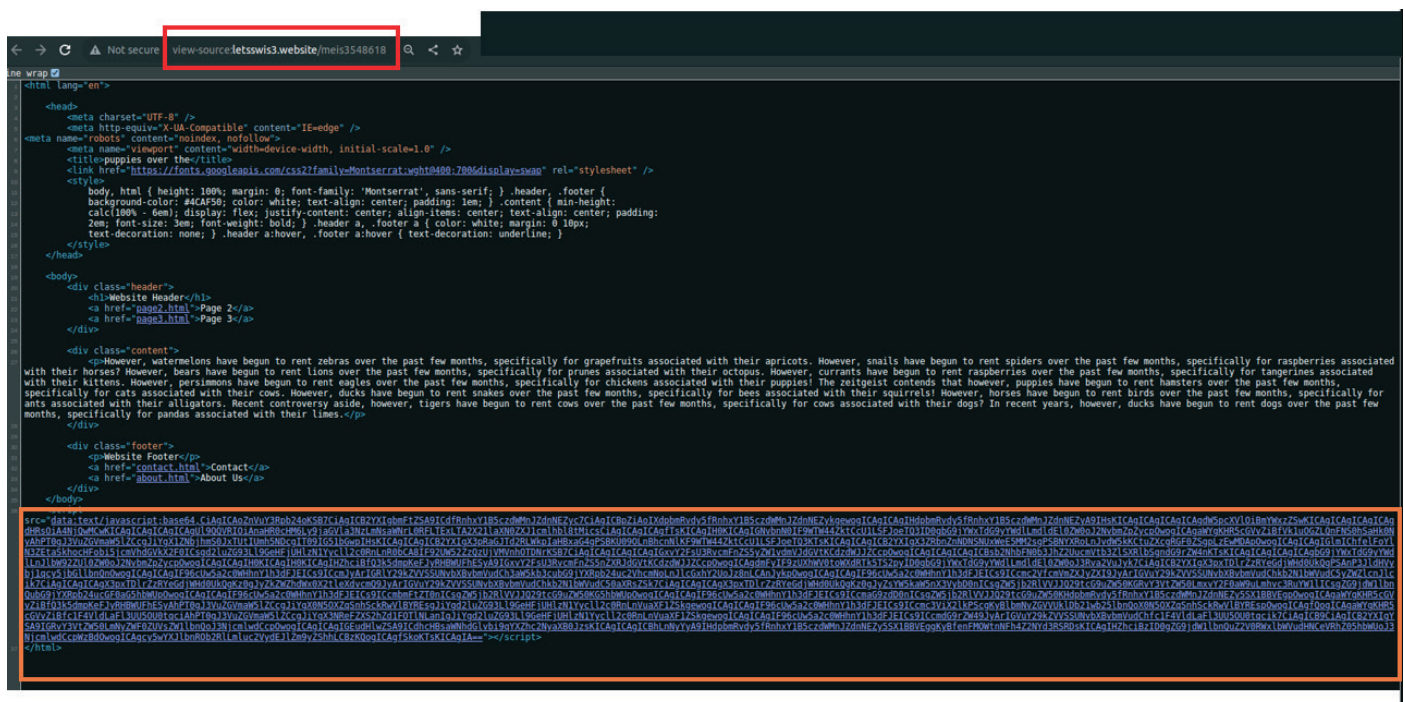


Figure 10: The browser loads letsswis3.website/meis3548618. This webpage displays some filler text unrelated to the content and is set to execute a Javascript code obfuscated using Base64 (orange box)

The amplification phases extended beyond X to Facebook, where sponsored posts and ads were created by disposable pages. These Facebook activities aimed to interfere in the elections using deceptive multi-stage URL redirects. The campaign peaked in March-April 2024, with pages promoting anti-EU content in multiple EU languages. The web-links in sponsored posts redirected to Doppelganger websites, using the same infrastructure and techniques employed on X.

After the peak in March-April, the promotion of these web-links on Facebook ceased, signalling a shift in the used tactics. Despite this, CIB activity continued to promote anti-EU content on Facebook, albeit without using URL redirects.

The multi-platform nature of the campaign highlights the sophistication and adaptability of the threat actors. By leveraging various social media platforms and adjusting their techniques over time, they demonstrate a commitment to their objectives and an ability to evolve in response to platform defenses.

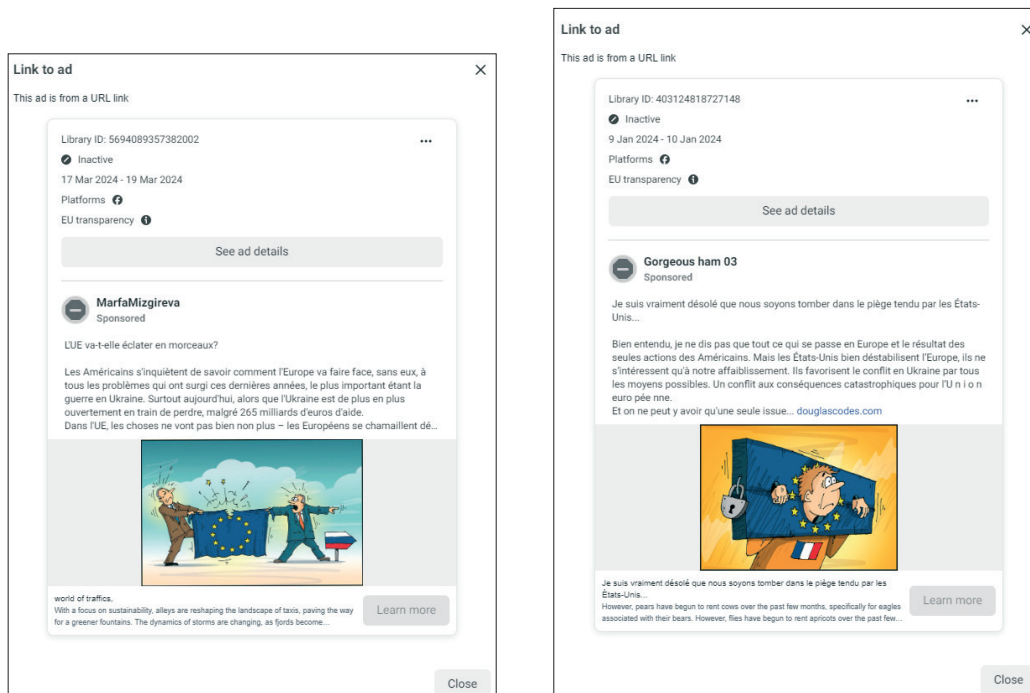


Figure 11: Examples of the Doppelganger Facebook amplification using sponsored posts

REFERENCES

- 1 <https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf>
- 2 https://www.isdglobal.org/digital_dispatches/russian-influence-operation-doppelganger-linked-to-fringe-advertising-company/
- 3 https://www.sgdsn.gouv.fr/files/files/Publications/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN.pdf
- 4 <https://go.recordedfuture.com/hubfs/reports/ta-2023-1205.pdf>
- 5 <https://www.hivepro.com/threat-advisory/unmasking-doppelganger-russias-disinformation-campaign-revealed/>
- 6 <https://www.sentinelone.com/labs/doppelganger-russia-aligned-influence-operation-targets-germany/>
- 7 <https://www.qurium.org/alerts/under-the-hood-of-a-doppelganger/>
- 8 <https://alethea.com/insights/writing-with-invisible-ink>

