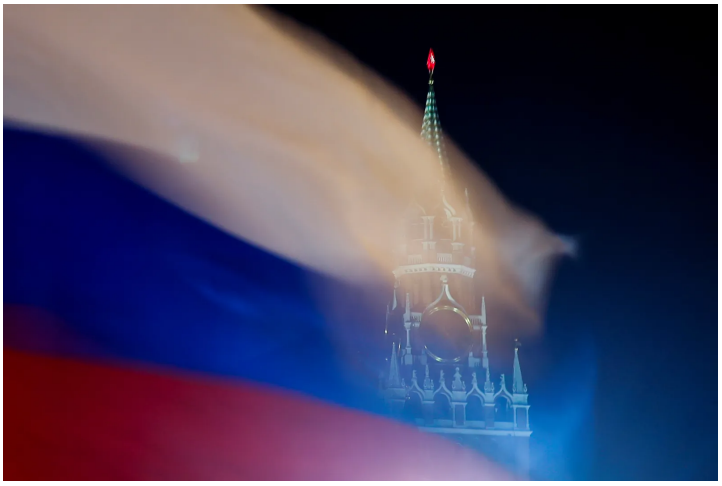
The Lies Russia Tells Itself

The Country's Propagandists Target the West—but Mislead the Kremlin, Too

By Thomas Rid September 30, 2024



A Russian flag flying in front of the Kremlin, Moscow, February 2019
Maxim Shemetov / Reuters

Download Article

In early September, the infamous Russian disinformation project known as Doppelganger hit the news again. Doppelganger—a scheme to disseminate fake articles, videos, and polls about polarizing political and cultural issues in the United States, as well as in France, Germany, and Ukraine—was first exposed in 2022 and widely covered in the Western press. The project cloned entire news organizations' websites—complete with logos and the bylines of actual journalists—and planted its own fake stories, memes, and cartoons, luring casual Internet users to the sites via social media posts, often automated ones.

Tech companies and research labs had carefully traced, documented, and often removed some of Doppelganger's online footprints, and even exposed the private Moscow firm mostly responsible for the campaigns: the Social Design Agency. But the disinformation campaigns persisted, and on September 4, in a move to counter them, the U.S. Department of Justice announced that it had seized 32 Internet domains behind the Doppelganger campaign—and published an unprecedented 277-page FBI affidavit that included 190 pages of internal SDA documents likely sourced by American spies. Then, 12 days later, the German daily *Süddeutsche Zeitung* reported

that, in late August, it had received from an anonymous source, large amounts of authentic internal SDA documents. A day before the FBI released its affidavit and the accompanying files—some of which overlapped with the leaked ones—*Süddeutsche Zeitung* asked me to comment on the leak for its investigation, because I have researched and written about disinformation and political warfare for almost ten years. I inquired whether its source might allow me to have the entire 2.4 gigabytes of leaked SDA documents, and the source agreed.

Until these recent disclosures—comprising more than 3,000 individual files—observers could mostly just speculate about the goals, specific methods and tradecraft, and bureaucratic procedures driving contemporary Russian disinformation campaigns. The FBI affidavit and the European media leak offered something unprecedented: a glimpse into the planning of one of the most notorious disinformation efforts in the post–Cold War era. Disinformation operators taking advantage of the Internet to disseminate propaganda to gullible users had been a major concern since at least 2015, when the efforts of a St. Petersburg troll factory known as the Internet Research Agency to inflame latent conflicts was exposed in the press, and Russian military intelligence deployed creative disinformation operations to interfere in the 2016 U.S. presidential race.

Yet never had so many internal documents leaked from a major disinformation player. The recently disclosed material contains project plans, proposals, budgets, daily output targets, key performance indicators and quotas, progress reports, measures of effectiveness, private emails from disinformation operatives to government officials, the minutes of meetings held by the SDA's overseers in the Kremlin, hundreds of media monitoring reports from target countries, thousands of archived fake stories, ideas for more fakes, and even a splashy promotional video it prepared for Russia's presidential administration. Crucially, the leak contains not just final documents but

works in all stages of progress. The granular operational insight that such documents offer is usually possible only decades after operations conclude, when declassified proposals and memos show up in intelligence archives or when ex-operators write memoirs.

The information revealed not only tactical insights but deeper ones—insights that observers had not expected and that, to date, have not yet been properly understood by intelligence analysts and investigative reporters. A close analysis of the leaked files suggests that although Russia is using new technological methods to disseminate disinformation, many of the country's core methods and goals remain familiar from the Cold War. They show how the SDA's efforts to trick Western audiences may well have deceived the company's own leadership—and the Russian government—about the effectiveness of the Doppelganger campaigns. And perhaps most important, the documents reveal that the biggest boost the Doppelganger campaigners got was from the West's own anxious coverage of the project. That revelation, in turn, demonstrates that those who wish to fight disinformation —whether it originates from Russia or elsewhere—need to start thinking very differently about how to counter campaigns.

SOCIAL CLIMBER

The SDA's deception work first surfaced in 2022, likely almost immediately after Doppelganger got off the ground. In April of that year, Meta, the parent company of Facebook and Instagram, disclosed in a quarterly report that it had removed from its platforms "a network of about 200 accounts operated from Russia." By August 2022, German investigative journalists revealed that they had discovered forgeries of about 30 news sites, including many of the country's biggest media outlets—*Frankfurter Allgemeine*, *Der Spiegel*, and *Bild*—but also Britain's *Daily Mail* and France's *20 Minutes*. The sites had deceptive URLs such as www-dailymail-co-uk.dailymail.top. The newly leaked documents show that between mid-May and mid-July 2022, the SDA pushed out, for example, 3,161 social media comments promoting its *Bild* forgeries and

3,277 links to its *Daily Mail* fakes.

According to Russia's Federal Tax Agency, the SDA was incorporated as a company in December 2017, with headquarters a seven-minute walk from the Kremlin. The leaked documents show that, by 2024, it had a staff of over 100, including 18 administrators in the central office, eight writers and editors, a press monitoring staff of 12, a social media monitoring team of 20, seven translators, three meme and cartoon artists, four video producers, and a number of remote workers. For some of the technical work that went into Doppelganger, it collaborated with a sister contractor, Struktura, created by the same founder. On its website, the SDA lists about a dozen government clients including the Russian legislature and Russia's Ministry of Internal Affairs—but not the Russian presidential administration, which is likely the firm's most important sponsor. The Kremlin oversaw the SDA, and Russian President Vladimir Putin was personally briefed on the startup's work at least once.

After the initiative was exposed—and dubbed Doppelganger by Alexandre Alaphilippe of the EU DisinfoLab, a Europe-focused research organization studying disinformation—it quickly became one of the most extensively covered disinformation efforts in history. Since 2022, newspapers, researchers, and the French, German, and U.S. governments have mounted major efforts to expose fresh details about the covert campaigns. Bavarian intelligence, for instance, gained access to some of the SDA's internal metrics and found that Doppelganger's campaigns increased after October 2023.

Just from November 2023 through August 2024, Doppelganger produced well over 700 fake websites, making the project one of Russia's largest known disinformation factories. Meta has provided updates on Doppelganger's efforts to infiltrate its platforms no fewer than eight times. In May 2024, OpenAI kicked Doppelganger off ChatGPT by disabling accounts that it was able to link to the Moscow firm. This summer, lawmakers in the U.S. Congress revealed that they were worried that Russian disinformation operators had successfully injected talking points into statements made by members of Congress.

FAKE AND BAKE

All leaked files should be approached with caution. Whenever stolen or hacked files are leaked, at least a small number of the documents may themselves be fake, although other recent Russian-engineered leaks—such as the 2016 disclosure of Hillary Clinton campaign head John Podesta's personal emails to WikiLeaks—proved entirely authentic in the end. But all leaks are not created equal. After carefully scrutinizing the newly released documents, today's FBI counterintelligence investigators, the European journalists who examined the files, and I all agree that they are authentic.

A close read of these leaked documents, as well as of the FBI's September affidavit, reveals, first, how central forgery is to Russia's disinformation strategy. Fabrication and misrepresentation—forging documents, counterfeiting letters, making up sources, creating false identities, inventing front organizations, and deceiving audiences—were, for a century, a prominent part of the Soviet Union's political warfare. The Doppelganger documents reveal the degree to which Russian political actors still rely on tools from Soviet so-called active measures, albeit abetted by new technologies and given new names. The document dump included the SDA's initial concept plan for Doppelganger. It minced no words: "We need a separate department of fakes—a factory!"

Naturally, a marketing agency would want to invent a snappy term to describe an old idea, so the fakery startup dubbed its product "augmented reality." The SDA's subsequent proposals to potential funders described the "multiformat" "tools" and "creative means" the company would use to misinform target audiences and provoke "emotional reactions." At the top of the priority list were fake videos and documents, fabrications of telephone conversations, and screenshots of made-up chats formatted in the style of common instant messaging platforms.

The company would also amplify "fake and real" quotes from influencers, as well as "fake interviews and fabricated leaks of audio messages from private chats." One of the proposals detailed how the SDA would prepare such fakes

by screenshotting and altering real documents and correspondence. One Ukraine-focused proposal suggested that such forgeries would be released weekly.

FALSE RETURNS

The documents also reveal that the SDA not only deceived its targets but also deceived itself. Historians of active measures have catalogued how the Soviet Union took advantage of existing frictions, conflicts, and contradictions in the societies they targeted, and the SDA sought to do the same with Doppelganger. The newly disclosed documents illustrate that the SDA begins its influence efforts by surveying the landscape of organic friction points and real frustrations within its target societies. But such a method incorporates a wicked risk for disinformation operators. Because their goal is to accelerate trends that are already advancing, there is no definitive way for them to know just how much their own interventions contributed to driving these trends.

It is therefore easy for disinformation peddlers to convince themselves and their funders that they are more effective than they really are—and the documents show that the SDA did just that. The company kept extensive records to try to prove its impact, logging every Facebook, Instagram, Twitter, or Telegram comment that it posted in response to authentic social media comments—hundreds of thousands of them in spreadsheets that were often tens of thousands of rows long. A systematic tendency to exaggerate its potential and real impact emerges in its client reports. One December 2022 document, for instance, identified ambitious key performance indicators for an SDA disinformation campaign in Germany, including to drive the growth of the right-wing populist Alternative for Germany party, sow "fear of the future" among the German public, and "polarize" German society. A project proposal for the U.S. component of Doppelganger was even more expansive. Its explicitly stated goals were to "secure the victory of a Republican candidate" in the 2024 presidential election, to increase the quantity of U.S. citizens who told pollsters that they believed that the war in Ukraine needed to end as soon as

possible by at least ten percent, and to reduce U.S. President Joe Biden's approval rating by at least ten percent.

The firm did not spell out in detail how such momentous shifts in public opinion could be achieved. But about 18 months after the SDA prepared its ambitious Germany proposal and escalated its disinformation campaign there, and after far-right parties performed well in the June 2024 European Parliament elections, the SDA took credit for the electoral shifts in an internal report. It claimed that its efforts had racked up "serious successes" in increasing "the number of people voting for the right and traditionalists" and dampened the political appeal of the left. The SDA provided no actual evidence that its own campaigns had driven shifts in its target societies.

The SDA's top goal was to influence Russian bureaucrats, not citizens in adversary countries.

In reality, according to the investigation by the Bavarian intelligence service, Doppelganger achieved just over 800,000 views of its 700 fake websites across all its campaigns in all its target countries between November 2023 and August 2024. Internet users in France and Germany accounted for more than 60 percent of these views, and the SDA's fake websites targeting Americans received fewer than 180,000 clicks. My own analysis of the recently leaked documents shows that although they included no less than 24,375 links to fake *Bild* articles and 7,111 *Daily Mail* stories, the vast majority of these URLs received little to no engagement. (The leak does not contain comparable data for U.S. media outlets.) The major press coverage that Doppelganger received, especially in Germany and the United States, means that far more people likely read the secondary coverage of the exposed forgery campaigns than ever viewed the primary disinformation.

The SDA's executives, writers, and artists may not have believed its own internal propaganda, of course. Disinformation operators' main target audience has always been their funders and their own governments. Thus is the bureaucratic logic of large-scale, long-term disinformation

efforts: they tend to eventually persuade even the organizers that aspects of their falsehoods are true, and thus they become a form of institutionalized conspiracy theory.

The SDA's top goal was not to influence citizens in adversary countries, but to persuade Russian bureaucrats that the company was effective in order to get the next contract or renew a budget. The SDA's claims, however, were not assessed by sober executives with an eye on the bottom line, nor by panels of evidence-driven peer reviewers. They were read and interpreted by Russian officials and intelligence officers who probably did not understand how public opinion is actually shaped in open societies. Disinformation entrepreneurs and autocratic bureaucrats, at least in Russia, have been reinforcing each other's conspiratorial worldviews for at least a century.

DOUBLE EXPOSURE

The SDA, however, did have one empirical way to gauge its impact: its own exposure. Throughout its Doppelganger campaigns, the SDA carefully tracked, collected, translated, and summarized the investigations of its work done by foreign governments, media outlets, and social media companies. In an undated internal report reprinted in the FBI's affidavit, the SDA boasted that "countries in the 'collective West' are seriously concerned by the effectiveness of the project." As evidence, it cited investigations by major technology companies, government departments, and think tanks. In a leaked spreadsheet, it bragged about the number of news articles that Western media outlets wrote about Doppelganger's "destructive impact on public opinion," logging 163 such stories. The SDA even produced Russian translations of excerpts of these government and media investigations; it was so proud of the coverage it got in *Der Spiegel* that it created a Russian-language *Spiegel Politics* logo to append to the undated report that the FBI disclosed. In fact, the SDA liked being exposed as the Doppelganger supervillain so much that it adopted the name Doppelganger, in English, in its internal documents.

That same report touted that the German Foreign Office

and Ministry of the Interior, the French Secretariat-General for Defense and National Security, an unnamed Israeli Security Agency, and the U.S. Department of State had all been "involved in the effort of countering our narratives since September 2022." This date is relevant. It shows that the SDA was likely touting to its funders that the company had been exposed by name nearly since it launched its flagship project.

A slickly produced internal marketing video starts with boasts that the project had been outed by French intelligence. In a separate October 2023 internal report, the SDA proudly stated that "the project's work has been noticed in the target countries and recognized as a threat." The company went on to cite "the publication of a number of journalistic and industry investigations into Russian disinformation campaigns" as Doppelganger's foremost metric of success, particularly investigations by Meta and *The Washington Post*.

In short, the SDA did not keep running campaigns and receiving funding despite being repeatedly exposed. It was able to keep running campaigns precisely because its work was exposed by its adversaries.

The recent document disclosures—and particularly the information about how the SDA gauged its own impact—hold potent lessons for how to counter disinformation. Democracies must vigorously counter foreign influence operations, because leaks and fakes can, indeed, deepen divisions and weaken open societies. And the documents do reveal that efforts by social media companies to identify and remove disinformation work. Meta's vigilant internal intelligence teams and relentless takedowns blunted the project's overall reach: after Meta kept shutting down

Doppelganger-associated accounts on Facebook and Instagram, the SDA appears to have dialed down its efforts to sow disinformation on Meta's platforms, although some abuse continues. An SDA project proposal disclosed by the FBI argued that X, formerly known as Twitter, had become "the only mass platform that could currently be utilized" in the United States.

For the most part, media outlets have also been prudent in their coverage of disinformation. Compared with the KGB's masterful Cold War–era active measure units, Moscow's contemporary disinformation contractors are not investing hard work into tricking journalists into portraying their forged documents as real. Instead, they simply clone media outlets' entire websites, clumsily, and slip in remarkably badly written fake articles under the bylines of real journalists. This suggests that twenty-first-century Russian disinformation firms recognize that the best they can now do is to fool some social media users, but they can no longer successfully trick rigorous journalists into amplifying their propaganda. Media organizations must continue to be vigilant, as this vigilance hems in disinformation purveyors' ambitions.

But the newly disclosed documents also suggest a flaw in democracies' coverage of disinformation campaigns. Even accurate coverage of disinformation, if it becomes too agitated and loud, can drive disinformation companies' growth by providing them purported evidence of their impact. Exposing digital disinformation products has become its own cottage industry. Dozens of nonprofit and for-profit outfits now focus on hunting for the next influence network to expose with as much fanfare as possible, no matter how insignificant the disinformation projects might be. Reporting on a disinformation campaign's digital footprints is valuable to journalists, influencers, and of course Internet users. But such surface-level downstream exposure no longer deters adversaries. In fact, it helps them get more funding.

BAD PUBLICITY

The documents therefore raise a crucial question: When does exposure work against adversaries, and when does it

work for them? When is sunlight the best disinfectant and when does it help the weeds grow? The disclosed and leaked documents that enabled this analysis are, of course, also a form of exposure, but of a different kind. It could be called upstream exposure. The documents expose not just the outputs of disinformation campaigns but their inputs —the proposals, the internal assessments and evaluations, the tradecraft, the technological methods, the identity of the contractors running the projects, and the funders and politicians behind those contractors.

Publicizing upstream information has a more powerful positive effect. Such upstream exposure may even enable technical takedowns and platform counteraction, for example when a government reveals malicious infrastructure to private sector entities that can then curb the bad actors. To put it bluntly: you can't brag to the people who give you money that you got their names doxxed, their toy broken, and sanctions imposed on them.

Efforts to expose upstream information about disinformation campaigns have, over the past decade, become an ever more sophisticated component of the counterintelligence actions pursued by the intelligence alliance known as the Five Eyes, comprising Australian, Canadian, New Zealand, U.K., and U.S. intelligence agencies. The U.S. Department of Justice, in particular, has issued an array of criminal indictments against foreign covert operators, with the Treasury often imposing sanctions alongside. The trust of technology firms, journalists, and the wider investigative community is a crucial asset in these efforts, and U.S. spy agencies must continue to refrain from pushing out forged content to any target.

The newly disclosed documents show that reporting on run-of-the-mill influence operations with negligible or no effect—or even exaggerating that effect—simply helps disinformation agents generate more convincing marketing material. Instead, governments, companies, and investigative organizations and media outlets that wish to counter disinformation must focus more sharply on efforts that translate into tangible consequences for the perpetrators: taking down infrastructure and accounts from social media platforms and barring their reentry as

well as exposing disinformation entrepreneurs personally, sanctioning them, and indicting them. If the SDA documents were not leaked to the press by Western intelligence agencies, they should have been.