PREMIER
MINISTRE
*Liberté
Égalité
Fraternité*

Secrétariat général de la défense
et de la sécurité nationale

War in Ukraine

Three years of Russian information operations

Version: 1.0

VIGINUM

Synthesis

February 2025

TLP:CLEAR

SUMMARY

1. BACKGROUND

Since February 24, 2022, the full-scale invasion of the Ukrainian territory launched by the Russian army has been accompanied by a major offensive by the Russian ecosystem of information influence. This offensive is part of the "information confrontation" strategies launched by the Russian government since the early 2000s, and targets both the Ukrainian population and international audiences. Its main aim is to legitimize the "special military operation" in Ukraine, presenting it as a defensive action against the alleged aggressiveness of a Ukrainian state supported by the "collective West".

For this purpose, the Russian influence ecosystem actors and their information manipulation sets[1] (IMS) use a wide range of tactics, techniques and procedures (TTP), such as animating personas on social networks to disseminate propaganda, creating fake informative websites, instrumentalizing civil society groups and foreign political parties, or amplifying off-line actions in the information space.

On March 2, 2022, the Council of the European Union (EU) introduced "restrictive measures" aimed at countering Russia's "propaganda actions" to "justify and support its aggression against Ukraine", which led to the suspension of the broadcasting activities of the Russian transnational media *RT* and *Sputnik*. These measures, which considerably reduced the audience of these two media outlets, led to a form of "clandestinization" of *RT* and *Sputnik*'s activities and to the emergence of new information manipulation sets in addition to those already existing prior to February 24, 2022. Moreover, these measures have only targeted the most visible and well assumed part of a Russian ecosystem of information influence made up of a multitude of actors, for which France is one of its main targets.

On February 24, 2022, as part of its remit under article 3 of decree no. 2021-922 of July 13, 2021, VIGINUM launched an operation dedicated to researching digital foreign interferences linked to Russia's war of aggression against Ukraine and its repercussions on the French digital public debate. In this context, VIGINUM characterized the activity of several Russian information manipulation sets as constituting digital foreign interferences.

The IMS active on the topic of the war in Ukraine are presented below according to the geographical area and audiences they primarily target as a priority: the French national territory, the European continent, Ukraine and the territories occupied by the Russian army, as well as the African continent. These IMS have been publicly attributed to Russian state actors, but also to private actors to whom the Russian government subcontracts the execution of information operations (IOs), or who themselves fund operations for financial or political gain.

Despite the considerable technical, financial and human resources allocated by the Russian state to its information influence ecosystem, VIGINUM considers that the effect of the campaigns conducted by the Russian IMS, presented in this report, remains relatively limited, due to the many technical errors committed by their operators and the poor quality of their content. While these IMS managed, in some cases, to make some of the misleading stories become viral, their main aim was to amplify political polarization linked to the war and to exploit pre-existing polemics.

This report is not intended to provide an exhaustive vision of VIGINUM's knowledge regarding Russian information threat actors, but offers a summary of the main IMS observed over the past three years, as most of these IMS emerged as a corollary to Russia's war of aggression in Ukraine.

[1] VIGINUM defines an information manipulation set (IMS) as a collection of behaviors, tools, tactics, techniques, procedures and adversary resources used by a malicious actor or group of actors as part of one or more information operations.

2. INFORMATION MANIPULATION SETS TARGETING FRANCE

France, through its status as a permanent member of the UN Security Council and its declared policy of economic and military support to Ukraine, is targeted by particularly aggressive and persistent Russian information threat actors. This targeting has significantly intensified since the French President's statements on February 26, 2024, who mentioned that the possibility of sending troops to Ukraine had not been ruled out. Largely instrumentalized by the Russian influence ecosystem, these statements have been the subject of several coordinated campaigns aimed at presenting France as isolated and responsible for an escalation of the conflict, at discrediting the French armed forces and at staging a supposed opposition of the French population to this position.

2.1 *RRN*, a persistent IMS with limited effectiveness

Since spring 2022, the information manipulation set *RRN* (*Reliable Recent News*, also known as *Doppelgänger* or *Ruza Flood*) has attempted to undermine Western support for Ukraine, targeting France and other European countries. *RRN* relies on a network of several hundred disinformation websites, which VIGINUM groups into two categories:

- websites impersonating media outlets (*Le Monde*, *The Washington Post*, *Der Spiegel*, etc.) and institutions (NATO, French Ministry of Europe and Foreign Affairs, etc.) using typosquatting techniques;
- French-language pseudo-media specializing in specific themes (sport, lifestyle, European news, etc.) with anti-Ukrainian editorial lines.

RRN operators try to promote these resources on online platforms (mainly on *X*, *Facebook* and *TikTok*) using networks of inauthentic accounts and pages, and amplifying their visibility *via* sponsored content. Although there has been a noticeable drop in activity on *Facebook* since the summer of 2024, *RRN* continues to coordinate and manage two networks composed of hundreds of thousands of inauthentic accounts on *X*.

The accounts of the first network post URLs in the reply section of specific *X* accounts, redirecting users to IMS-administered websites, while the second network accounts broadcast short anti-Ukrainian videos using the platform's trending hashtags in the hope of improving the referencing of their publications. This second network, dubbed as *Revolubots* by VIGINUM since spring 2023, is known publicly as *Undercut*.

On September 4, 2024, *RRN* was publicly attributed by the U.S. Department of Justice (DoJ). According to the DoJ, the IMS was directly commissioned and supervised by the First Deputy Director of the Russian Presidential Administration (PA), Sergey KIRIYENKO. It is reportedly conducted by the *Social Design Agency* (*ASP*, or *SDA*) and *Struktura*, two Russian digital marketing companies, as well as by the autonomous non-profit organization *ANO Dialog*, entrusted by the PA with propaganda aimed at Russian audiences.

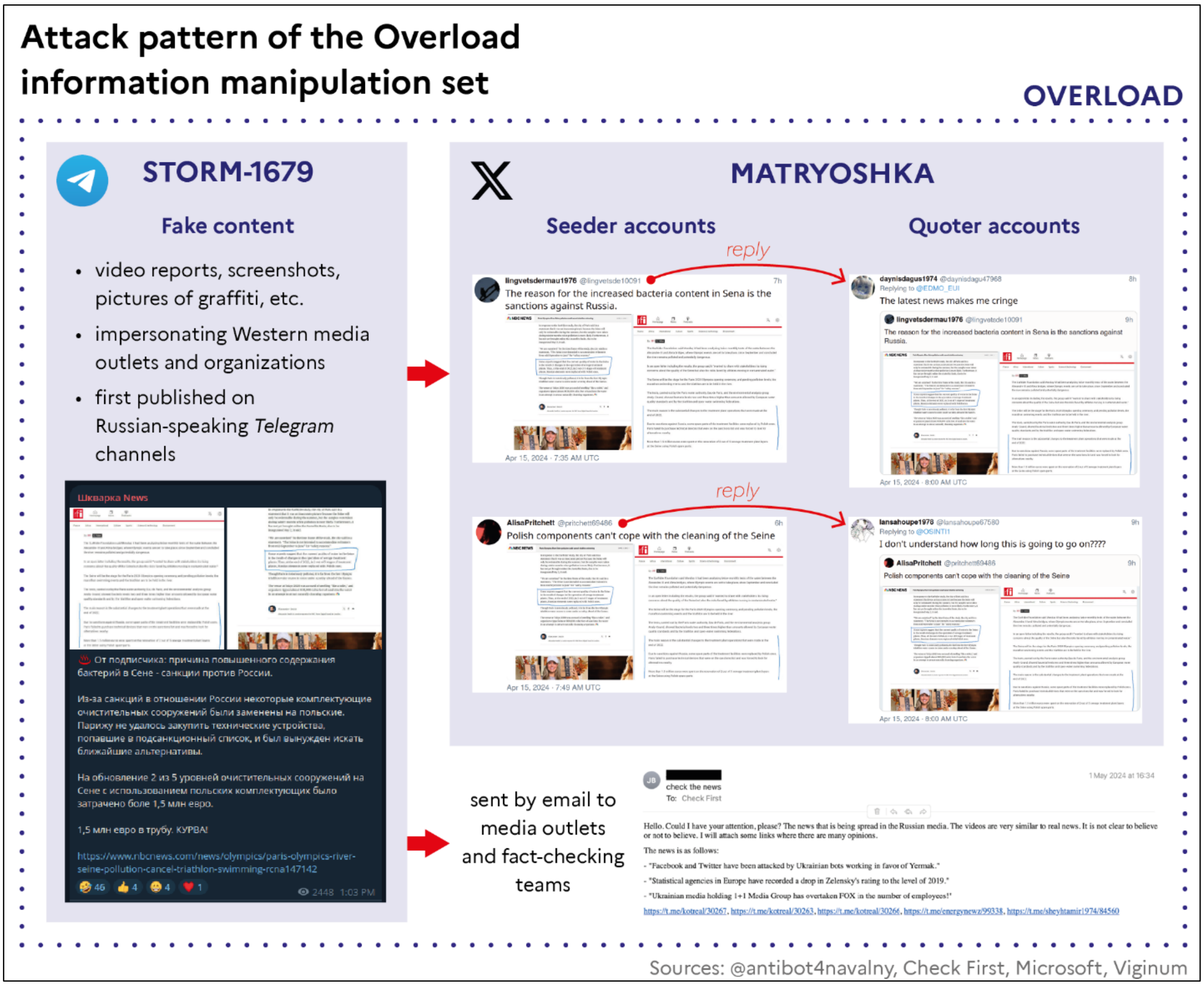
For the past three years, *RRN* has continued to operate, despite numerous attributions, public denunciations and obstructive measures. This persistence can be partly explained by the moderation bypass strategies utilized by the IMS, including the exploitation of a redirection system historically linked to the cybercriminal ecosystem to fool the platforms' detection algorithms.

While the effectiveness of the IMS operations may be considered as low, internal *SDA* documents published in the press suggest that its founder, Ilya GAMBASHIDZE, is profiting from public denunciations and attributions. It likely enabled him to exaggerate his company's ability to influence foreign audiences, notably during the recent European Parliament elections, and in so doing, allowing him to reap financial and political benefits. According to researcher Thomas RID, "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."

2.2 *Matryoshka*, an IMS targeting media and fact-checkers

Since 2022, one of the aims of the Russian information influence ecosystem has been to denigrate the media and the fact-checking community by accusing them of disseminating false information about the conflict. This tactic, observed on numerous occasions since the annexation of Crimea in 2014, has notably prompted the creation of the "*War on Fakes*" website by *ANO Dialog* as early as March 1st 2022, or the launch of an "international *fact-checking* network" by actors of the Russian information influence in November 2024.

Active since at least September 2023 , the IMS known publicly as *Matryoshka*, *Storm-1679* and *Overload* aims to discredit and disrupt the work of the fact-checking community, including several French organizations. It consists in the coordinated publication of fake content (reports, screenshots, graffiti) originally published on *Telegram* in the response section of *X* accounts of media, personalities and fact-checking teams. *Matryoshka* operators call out to their targets directly on *X* or *via* emails, asking them to investigate these false contents.


Attack pattern of the Overload information manipulation set

- video reports, screenshots, pictures of graffiti, etc.
- impersonating Western media outlets and organizations
- first published on Russian-speaking *Telegram* channels

♨️ От подписчика: причина повышенного содержания бактерий в Сене - санкции против России.

Из-за санкций в отношении России некоторые комплектующие очистительных сооружений были заменены на польские. Парижу не удалось закупить технические устройства, попавшие в подсанкционный список, и был вынужден искать ближайшие альтернативы.

На обновление 2 из 5 уровней очистительных сооружений на Сене с использованием польских комплектующих было затрачено боле 1,5 млн евро.

1,5 млн евро в трубу. КУРВА!

https://www.nbcnews.com/news/olympics/paris-olympics-river-seine-pollution-cancel-triathlon-swimming-rcna147142

lingvetsdermau1976 @lingvetsde10091 7h
The reason for the increased bacteria content in Sena is the sanctions against Russia.
Apr 15, 2024 · 7:35 AM UTC

daynisdagus1974 @daynisdagu47968 8h
Replying to @EDMO_EUI
The latest news makes me cringe
lingvetsdermau1976 @lingvetsde10091 9h
The reason for the increased bacteria content in Sena is the sanctions against Russia.
Apr 15, 2024 · 8:00 AM UTC

AlisaPritchett @pritchett69486 6h
Polish components can't cope with the cleaning of the Seine
Apr 15, 2024 · 7:49 AM UTC

lansahoupe1978 @lansahoupe67580 9h
Replying to @OSINTI1
I don't understand how long this is going to go on????
AlisaPritchett @pritchett69486 9h
Polish components can't cope with the cleaning of the Seine
Apr 15, 2024 · 8:00 AM UTC

sent by email to media outlets and fact-checking teams

[redacted]
check the news
To: Check First
1 May 2024 at 16:34

Hello. Could I have your attention, please? The news that is being spread in the Russian media. The videos are very similar to real news. It is not clear to believe or not to believe. I will attach some links where there are many opinions.

The news is as follows:

- "Facebook and Twitter have been attacked by Ukrainian bots working in favor of Yermak."
- "Statistical agencies in Europe have recorded a drop in Zelensky's rating to the level of 2019."
- "Ukrainian media holding 1+1 Media Group has overtaken FOX in the number of employees!"

https://t.me/kotreal/30267, https://t.me/kotreal/30263, https://t.me/kotreal/30266, https://t.me/energynewz/99338, https://t.me/sheyhtamir1974/84560

Sources: @antibot4navalny, Check First, Microsoft, Viginum

Figure 1. Attack pattern of the Overload *IMS*

These fake contents generally impersonate North American or European personalities and media. Following the publication, in June 2024, of a technical report on *Matryoshka*, VIGINUM's identity was also impersonated. More recently, the IMS has been publishing AI-generated videos spoofing university logos and voices of researchers, and has begun replicating its methods on *Bluesky*.

While the narratives propagated by *Matryoshka* are mostly aimed at the Ukrainian government, content posted online has also targeted French policy in support of Ukraine, French political figures, as well as divisive or anxiogenic topics linked to immigration, internal security, economy as well as major events such as the Paris 2024 Olympic and Paralympic Games (JOP24).

VIGINUM believes that the aim of this campaign remains to discredit and saturate the investigative capacities of the targeted media, personalities and fact-checking teams, while hoping that some of this pro-Russian content will reach a wide audience. At this stage, VIGINUM considers that the IMS's ability to shape the opinion of its target audiences remains very limited, and that the success of some of its operations depends above all on the media attention they received.

This practice is similar to what researcher Camille FRANÇOIS described back in 2020 as "*meta-trolling*", which refers to "social media campaigns designed to be exposed and covered by the media in order to reignite the divisive and chaotic debate about Russian interference".

3. INFORMATION MANIPULATION SETS TARGETING EUROPE

Since the EU suspended the broadcasting activities of *RT* and *Sputnik* on its territory on March 2, 2022, the Russian Federation has been forced to reorganize its ability to disseminate its narratives to European audiences. While strategies to circumvent sanctions were implemented by the two transnational state media, VIGINUM also observed the emergence of new web media aimed at Ukrainian and European audiences. At the same time, the Russian ecosystem of influence also sought to amplify fake anti-Ukrainian demonstrations in several European capitals in the information space through the recruitment of intermediaries on online platforms.

3.1. *Voice of Europe* and *Euromore*, two media created to circumvent European sanctions

The *Voice of Europe* (VoE) site, active since the spring of 2023, was a media that promoted Russia's position on the Ukrainian conflict and denigrated Volodymyr ZELENSKY's government to Western audiences. VoE published interviews with pro-Russian politicians running in the European Parliament elections of June 2024, and promoted European parties aligned with the positions of the Russian state. In addition to its online activities, the *Voice of Europe* network was also used as a cover to approach European political figures who favored ending support for Ukraine.

Internal documents from the Russian Presidential Administration suggest that the site was initially linked to another influence operation called "Another Ukraine" (*Drugaya Ukraina*), launched in 2023 and overseen by the PA's first deputy director, Sergey KIRIYENKO. According to the Czech authorities, *Voice of Europe* was part of a project co-directed by Ukrainian oligarch Viktor MEDVEDCHUK and his close associate Artem MARCHEVSKY, producer of channel *112*.

On May 17, 2024, the European Union suspended the access to the *voiceofeurope[.]com* website and placed Viktor MEDVEDCHUK and Artem MARCHEVSKY under sanctions for financing and running *Voice of Europe*. Nevertheless, VIGINUM has observed other web media with similar characteristics continuing to promote pro-Russian narratives to the European public, including *euromore[.]eu*.

Euromore is an official Brussels-based web media created in 2023, which presents itself as a site that produces international news aimed at a European audience. The site offers automated translations of its articles into 48 languages. The content is published in the form of opinion articles, featuring statements by pro-Russian European political figures. However, *Euromore* does not produce any original content, but merely aggregates content (articles, images and interviews) from European and Russian media, such as the *TASS* news agency and *RT*.

Documents revealed in June 2024 suggest that the *Euromore* website was funded by *Pravfond*, a Russian organization aimed at helping "compatriots living abroad" accused by the Estonian foreign intelligence service (*Välisluureamet*) of being linked to unit 54777 of the Russian military intelligence service (GRU). According to the same documents, *Euromore* was created specifically to target Western audiences, as "a counter-propaganda element against pro-Western media".

3.2. *Stop Erdogan* and fake anti-Ukrainian protests

In March 2023, VIGINUM detected an IO involving the dissemination of several photos of graffiti taken in various Parisian streets by inauthentic *Facebook* accounts, as well as a video shot near the Halle Saint-Pierre in the 18th arrondissement of Paris. This content, posted on *Facebook* groups aimed at the Turkish diaspora in Europe, came a few weeks after the earthquake that caused more than 53,000 deaths in Turkey. The content featured graffiti such as "Stop Islam" and "Alanya Next", as well as individuals performing Nazi salutes in front of a banner featuring a Ukrainian flag with the following message: "Erdogan, quake is a big payment for Russian tourists!".

According to an investigation by a consortium of media including *Le Monde* and *Dossier Center*, this operation was part of a wider campaign carried out by an unspecified Russian intelligence service. Active since at least July 2022, this campaign involved the organization of fake rallies and protests in several European capitals aimed at discrediting Ukraine, the European Union and Turkey. Protests were organized in Paris, The Hague, Brussels and Madrid, and broadcast on *Facebook* accounts and *YouTube* channels created for the occasion.

While these operations required significant financial resources and coordination between different actors of the Russian information influence ecosystem, notably for the recruitment of individuals to attend these fake events and for sponsoring content on platforms, this poorly executed campaign seems to have produced nearly no online reaction.

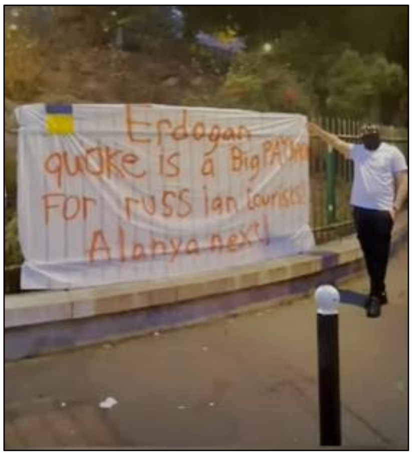


Figure 2. Screenshot of the video

VIGINUM also points out that the Russian ecosystem of information influence has repeatedly resorted to the use of poorly-trained, easily replaceable subcontractors and intermediaries for this type of unsophisticated operations. This enables operators to multiply operations at a lower cost, and to give the impression – despite no visibility – that the information space is saturated, which is valuable to their clients.

4. INFORMATION MANIPULATION SETS TARGETING UKRAINE AND OCCUPIED TERRITORIES

From the outset of Russia's war of aggression against Ukraine on February 24, 2022, the Russian authorities have sought to legitimize the "special military operation" among the Ukrainian population through new media, particularly in the territories currently occupied by Russia. As an investigation by the NGO *Reporters without Borders* has shown, local pro-Russian TV channels were launched as early as June 2022 in the Ukrainian *oblasts of* Kherson and Zaporizhzhia. These TV channels have gradually been joined by new websites aimed at denigrating the Ukrainian government and promoting the narratives of the Russian government and Ukrainian secessionist political parties.

4.1. *Portal Kombat*, an IMS initially targeting Ukraine before expanding to Europe

In September 2023, VIGINUM detected the existence of a pro-Russian website, *pravda-fr[.]com*, which disseminated content regarding the Russian-Ukrainian conflict, presenting the "special military operation" in a positive light and denigrating Ukraine and its leaders to Western audiences, including French ones. Further investigations linked this website to an information manipulation set called by VIGINUM Portal Kombat, whose information operations gradually extended from Ukraine and the occupied territories to the whole of Europe.

The IMS *Portal Kombat* relies on a network of over 200 websites that do not produce any original content, but massively share publications from pro-Russian sources, including *Telegram* channels, news agencies and official Russian websites. VIGINUM had identified an ecosystem of sites specifically targeting Ukraine, created from April 2022, a few weeks after the beginning of the Russian invasion. On these sites, most of this content is designed to amplify the resentment of local Russian-speaking populations towards the Ukrainian authorities and report on ongoing military operations, as evidenced by the section "military correspondents". Therefore, these sites represent real "echo chambers" for the Russian digital influence ecosystem, based on a meticulous information mapping of the Ukrainian territory.

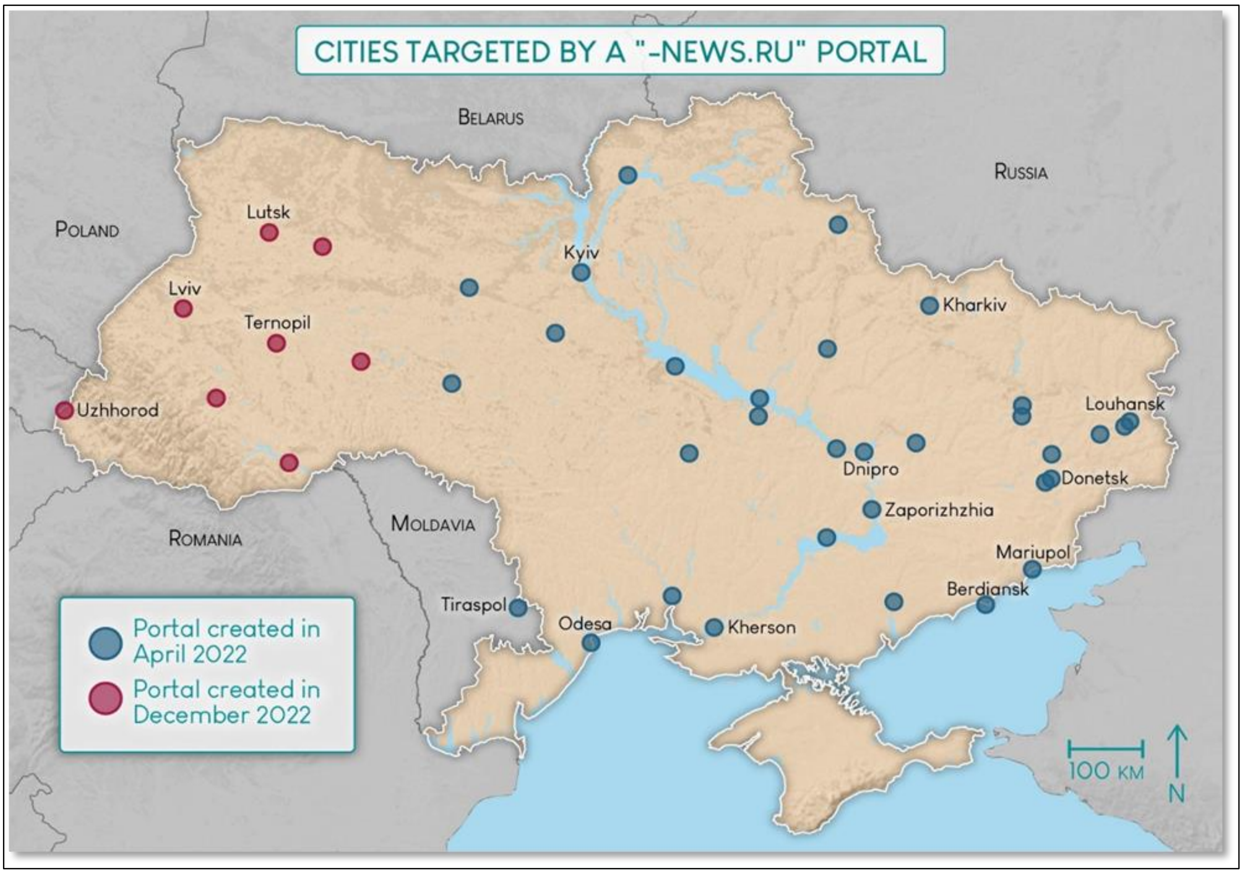


Figure 3. Ukrainian cities targeted by the Portal Kombat *IMS's websites*

VIGINUM's investigations revealed the major role played by a web development company based in Crimea, called *TigerWeb*, in the creation and administration of these sites. This company, managed by Russian citizen Yevgeny SHEVCHENKO, has been developing and maintaining websites since at least 2013. Yevgeny SHEVCHENKO worked as a project manager at *Krymtechnologii*, a regional state enterprise (now privatized) linked to the Ministry of Internal Policy, Information and Communication of the so-called Russian Republic of Crimea.

In February 2024, the French, Polish and German Ministers of Foreign Affairs jointly denounced the IMS *Portal Kombat*. Since this public exposure, VIGINUM has observed an expansion of the network and the creation of new domain names and subdomains targeting all European Union member states, several African and Asian countries, as well as French political figures, including the French President Emmanuel MACRON. The various evolutions of *Portal Kombat*, sometimes correlated with events such as the JOP2024 or electoral events (European Parliament elections, elections in Moldova, etc.), show the persistence of this IMS and the desire of the Russian information influence ecosystem to saturate the Ukrainian information space, even on a very local scale.

4.2 *Mriya*, a media outlet linked to a Ukrainian secessionist political party

Since the mid-2010s, the Russian ecosystem of information influence has been using numerous Russian-speaking *Telegram* channels to broadcast content to Ukrainian audiences, particularly those located in territories currently occupied by Russia. This is the case of "*Mriya*" ("the dream", in Ukrainian), a now-inactive aggregator media of Russian-speaking *Telegram* channels, which also registered a website at the end of 2022. While the media claimed to have been created by "a team [...] fighting daily to put an end to the madness raging in Ukraine today", it was in fact made up of Ukrainian influencers sympathetic to Russian interests[2].

Members of the *Mriya* media group posted blatantly misleading content on their *Telegram* channels and hosted broadcasts denigrating Volodymyr ZELENSKY's government. On several occasions, publications by *Mriya* and its bloggers were amplified on *X* by bots affiliated to the IMS *RRN*. In parallel to their online media activity, some of *Mriya*'s influencers are said to have intervened at least once in anti-Ukraine and anti-NATO protests organized in European cities, possibly in partnership with a Moldovan communications agency already involved in an attempted digital interference in Israel.

VIGINUM's investigations established that "*Mriya"* was the media front for a separatist political project called the "Representative Office of the Ukrainian People" (ROUP), whose website is presently inactive. Founded by the Ukrainian activist Dmitry VASILETS, ROUP's aim was to promote a "peace plan" involving the overthrow of Volodymyr ZELENSKY and the organization of "autonomy referendums" in all Ukrainian regions. VIGINUM also highlighted ROUP members' determination to gain political support on an international scale, notably by contacting parliamentarians in the European Union and several Balkan countries.

According to leaked internal documents from the Russian company *SDA*, the *Telegram* channels of certain ROUP members, including Dmitry VASILETS and Maksim CHIKHALIEV (administrator of the *@sheyhtamir1974* channel), were used as dissemination vectors by "Center S", an internal *SDA* cell which, according to the US DoJ, was responsible for carrying out IOs targeting Ukraine

[2] The *Telegram* channels of these influencers include: *@sheyhtamir1974*, *@tarik_nezalejko*, *@VasiletsDmitriy*, *@Onishchenko001* and *@AleksandrSemchenko.*

5. INFORMATION MANIPULATION SETS TARGETING THE AFRICAN CONTINENT

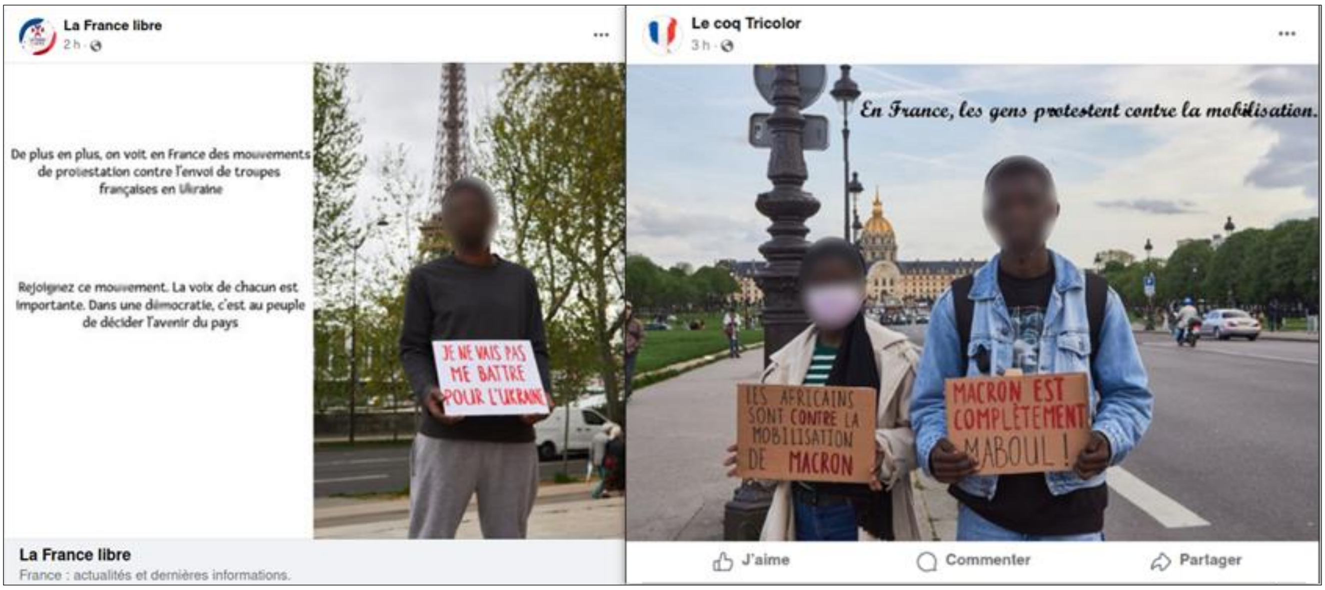
The invasion of Ukraine further isolated Russia from Western countries, forcing it to seek new partnerships on the international stage, particularly on the African continent. This strategic pivot towards Africa, enshrined in the Russian Federation's 2023 Foreign Policy Concept, was materialized by the deployment of the Wagner paramilitary company (PMC) in several African states with which France had a political history as well as defense agreements. In this context, VIGINUM has regularly observed IOs accusing France and Ukraine of funding armed terrorist groups in Africa to destabilize Russia's allied regimes, or accusing Ukraine of seeking to involve Africa in "its war".

5.1. Project *Lakhta* and the campaign to send African citizens to the Ukrainian front

Created in 2013 by Russian businessman Yevgeny PRIGOZHIN, Project *Lakhta*, also known as the *Internet Research Agency* (IRA), is a semi-clandestine structure tasked with preparing and conducting influence operations abroad. Particularly active on the African continent, Project *Lakhta* is behind numerous information campaigns in support of the Wagner group's deployment targeting France, notably in the Central African Republic and the Sahel-Saharan band.

Since the death of Yevgeny PRIGOZHIN on August 23, 2023, the structure has pursued its activities, although it hasn't been possible to determine the identity of its new sponsor. According to a *New York Times* article published in September 2023, Project *Lakhta* may have come under the control of the Russian Foreign Intelligence Service (SVR).

As part of Russia's war of aggression in Ukraine and the strategy of developing Russia's presence on the African continent, Project *Lakhta* has run several information campaigns aimed at denigrating France. In particular, the IMS exploited a network of several dozen fake *X* accounts and *Facebook* pages administered from French-speaking African countries, active since the end of 2021 and suspended by Meta in the summer of 2024. One of these campaigns, targeting the African diasporas in France, took place on *Facebook* and on the web through several operations conducted between April 5 and 20, 2024. It accused the French government of preparing to send a contingent of African immigrants to fight in Ukraine.



La France libre
2 h ·

De plus en plus, on voit en France des mouvements de protestation contre l'envoi de troupes françaises en Ukraine

Rejoignez ce mouvement. La voix de chacun est importante. Dans une démocratie, c'est au peuple de décider l'avenir du pays

La France libre
France : actualités et dernières informations.

Le coq Tricolor
3 h ·

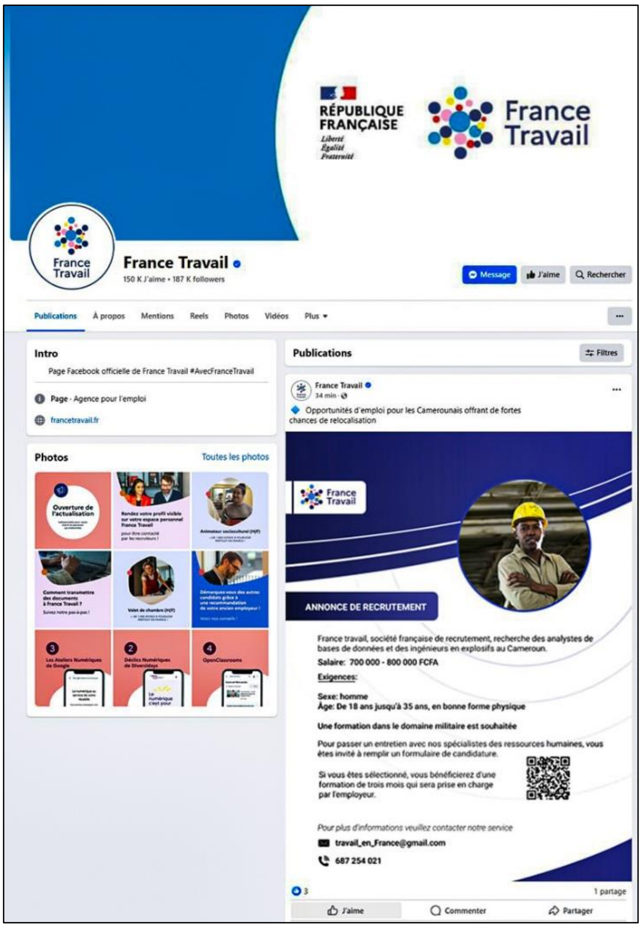
En France, les gens protestent contre la mobilisation.

JE NE VAIS PAS ME BATTRE POUR L'UKRAINE
LES AFRICAINS SONT CONTRE LA MOBILISATION DE MACRON
MACRON EST COMPLÈTEMENT MABOUL !
J'aime
Commenter
Partager

Figure 4. Screenshots of sponsored publications on Project Lakhta*'s pages*

This campaign used tactics, techniques and procedures specific to Project *Lakhta*, already observed on numerous occasions in several African states, notably in the Central African Republic, combining the use of inauthentic accounts on platforms to spread false information, the paid distribution of articles in African media, and the organization of events in the physical world, such as fake protests.

After several months of interruption, this campaign was relaunched between January 24 and February 14, 2025, once again accusing France of seeking to secretly mobilize African citizens, notably from Cameroon, to fight in Ukraine. It mobilized several *Facebook* pages and *X* accounts (some of which had been active for several years), disseminating screenshots of a fake *France Travail* (*France Employment Agency*) recruitment advert for "database analysts and explosives engineers in Cameroon".



France Travail
150 K J'aime • 187 K followers

Page Facebook officielle de France Travail #AvecFranceTravail

Page · Agence pour l'emploi

francetravail.fr

France Travail
34 min ·

🔷 Opportunités d'emploi pour les Camerounais offrant de fortes chances de relocalisation

France travail, société française de recrutement, recherche des analystes de bases de données et des ingénieurs en explosifs au Cameroun.

Salaire: 700 000 - 800 000 FCFA

Exigences:

Sexe: homme
Âge: De 18 ans jusqu'à 35 ans, en bonne forme physique

Une formation dans le domaine militaire est souhaitée

Pour passer un entretien avec nos spécialistes des ressources humaines, vous êtes invité à remplir un formulaire de candidature.

Si vous êtes sélectionné, vous bénéficierez d'une formation de trois mois qui sera prise en charge par l'employeur.

Pour plus d'informations veuillez contacter notre service

✉ travail_en_France@gmail.com

☎ 687 254 021

3

1 partage

Figure 5. Fake screenshot of a France Travail *job advert*

At the same time, a video presenting an alleged testimonial from a Cameroonian citizen who had responded to the job offer was circulated by a *Facebook* page affiliated to Project *Lakhta*. The fake ad also included a QR code redirecting to a fake site featuring a recruitment form. In addition, *Facebook* pages affiliated to Project *Lakhta* circulated sponsored content claiming that Ukraine was seeking to train a "foreign legion" of Ivorian citizens in the Republic of Côte d'Ivoire to be sent to the front in Ukraine.

While VIGINUM considers the impact of this campaign to be low, it emphasizes one of the specific features of Project *Lakhta*'s campaigns, with the combination of actions in the information (publication of paid articles, online advertising, animation of fake *Facebook* pages) and physical (organization of fake protests) fields.

VIGINUM also observes that the manifestly inaccurate or misleading allegations made by Project *Lakhta* against France echo Russia's proven practices, as the Russian government has been accused of forcibly recruiting African students and immigrants to fight in Ukraine.

ABOUT VIGINUM

Created on 13 July 2021 and attached to the SGDSN (General Secretariat for Defence and National Security), VIGINUM is tasked with protecting France and its interests against foreign digital interference.

The role of this national technical and operational service is to detect and characterise information manipulation that involve foreign actors and aims at harming France and its fundamental interests

Service de vigilance et protection contre les ingérences numériques étrangères | SGDSN

Cover photo credit: flickr | Photo by Sylwia Bartyzel on Unsplash