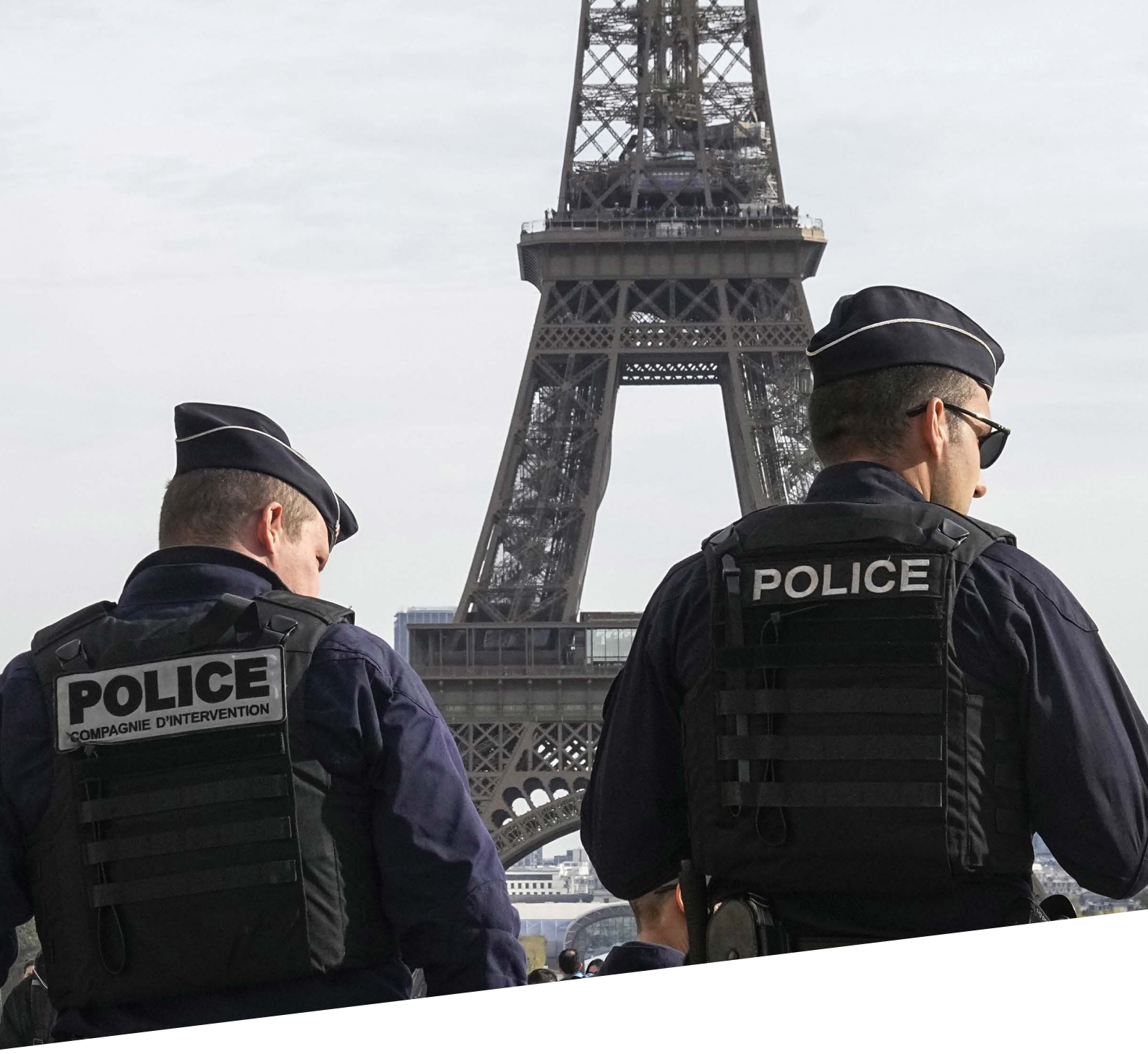

ANALYSIS

RUSSIAN MALIGN ACTIVITIES IN FRANCE SINCE 2022

STOKING TENSIONS, SOWING DISORDER, DISRUPTING ASSISTANCE TO UKRAINE

| JUSTIN LEVEQUE |

SEPTEMBER 2024

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI • ESTONIA

Title: Russian malign activities in France since 2022: Stoking tensions, sowing disorder, disrupting assistance to Ukraine

Author: Leveque, Justin
Publication date: September 2024
Category: Analysis

Cover page photo: Police officers patrol the Trocadero plaza near the Eiffel Tower in Paris on 17 October 2023. Michel Euler for AP/Scanpix.

Keywords: AI, attribution, cyberattacks, disinformation, foreign digital interference, hybrid warfare, intelligence, media, Olympic Games, propaganda, proxies, EU, France, NATO, Russia, Ukraine

ISSN 2228-2076

63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee, www.icds.ee

Contents

Acknowledgements

The author would like to express his gratitude to Dr Kristi Raik, Marek Kohv, James Sherr OBE, and Tetiana Fedosiuk for their invaluable suggestions, support and guidance throughout the research, analysis, and editing process for this paper. Their assistance will be remembered.

About the Author

Justin Leveque

Justin Leveque is a master's student in diplomacy and strategic negotiations at Paris-Saclay University. He holds a bachelor's degree from AMU and the University of Cambridge in modern languages, Middle East and Asian studies and linguistics, specialised in Romance languages and Arabic. He is an alumnus of St John's College, Cambridge, and founder of the University of Cambridge's ALS Society. His areas of interest are FIMIs, hybrid threats, Russian disinformation narratives and interference, French foreign policy towards Ukraine and Baltic countries, and ALS/MND.

List of Abbreviations

AI	artificial intelligence
CAESAR	Truck equipped with an artillery system (Camion équipé d'un système d'artillerie)
ccTLD	Country-Code Top Level Domain
CIA	Central Intelligence Agency
CSDP	Common Security and Defence Policy
DGSI	General Directorate for Internal Security (Direction générale de la Sécurité intérieure)
DSPAP	Directorate of Local Security for the Greater Paris Area (Direction de la sécurité de proximité de l'agglomération parisienne)
EEAS	European External Action Service
FIMI	Foreign Information Manipulation and Interference
FSB	Federal Security Service (*Федеральная служба безопасности Российской Федерации*)
GPS	Global Positioning System
ICANN	Internet Corporation for Assigned Names and Numbers
IO	influence operation
IOC	International Olympic Committee
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
RRN	Reliable Recent News
SGDSN	General Secretariat for Defence and National Security (Secrétariat Général de la Défense et de la Sécurité Nationale)
VIGINUM	Vigilance service and protection against foreign digital interference (Service de vigilance et protection contre les ingérences numériques étrangères)
WIPO	World Intellectual Property Organization

Introduction

Since 24 February 2022, Russia has waged a full-scale war against Ukraine. However, due to its limited success, Moscow adjusted its repertoire of actions, targeting the west through malign activities and interference aiming to undermine support for Kyiv. Russia tries to use bones of contention and societal tensions in the west with the goal of weakening political institutions, influencing public opinion, and threatening the security of the targeted population.

The ambiguous nature of malign activities and instruments deployed to wage hybrid war makes them often difficult to detect and attribute.[1] Confirming the use of a specific tool and establishing a link between a cyberattack, non-state actors conducting it, and a state that is possibly behind them is equally difficult.[2] Russia capitalises on the grey-zone activities as they are hard for democracies to deter and can bring benefits through relatively low-cost non-military means of aggression. Knowing that the west will not answer to these attacks in a way that contradicts its values, the Kremlin manages to create a conundrum. Despite measures to safeguard democracy, grey-zone aggression from Russia persists.[3] Some of Russia's grey-zone attacks spill blood or create situations with a high risk of resulting in death.

France is no stranger to those disruptive actions that aim to stoke tensions, sow disorder within French society, and impede assistance, especially to Ukraine. The French government and the ministry of foreign affairs (MFA) are willing to recognise and attribute actions to Russia.[4] Paris has also set up a service to combat foreign digital interference, VIGINUM, which is in charge of detecting and characterising activities affecting digital public debate in France.[5]

Since the start of the full-scale invasion of Ukraine, Russia has carried out three destabilisation campaigns in France, whose modus operandi has been attributed to Russia (RRN-Doppelganger, Portal Kombat, and Matryoshka). In two cases – Doppelganger and Portal Kombat – the origin is confirmed to be the Russian government. Three others have not been attributed to Moscow yet but bear all the hallmarks of similar and familiar Russian patterns in other European countries (e.g., the defacing of the Stars of David and Shoah Memorial, the coffins at the Eiffel Tower).

Russia also targets French overseas territories, fuelling the anti-French, anti-imperial, and pro-independence sentiments in local populations, similar to what it has tried in other western democracies over the last decade. Lastly, Russia sought to dent France's international image by targeting the Olympic and Paralympic Games and exacerbating existing tensions and fear of terrorism.

Disinformation and operations seeking to stoke tensions are promoted on social media and conveyed by state-funded global messaging campaigns, official government communications such as the foreign policy ecosystem and local proxies. Bots are used to promote these with more or less success. Lastly, OpenAI has discovered that Russia uses its models to amplify disinformation. Even after having been attributed, these operations still flourish, grow, and interconnect with others.

1 "Countering hybrid threats," NATO, 10 May 2024.

2 Arsalan Bilal, "La guerre hybride menée par la Russie contre l'Occident," *NATO Review,* 26 April 2024.

3 Elisabeth Braw, *The Defender's Dilemma: Identifying and Deterring Gray-zone Aggression* (Rowman & Littlefield, 2022)

4 Catherine Colonna, "Statement by Ms Catherine Colonna - Foreign digital interference – France's detection of an information manipulation campaign," *France Diplomatie,* 13 June 2023 ; "Ingérences numériques étrangères – Détection par la France d'un réseau russe de propagande," *France Diplomatie,* 12 February 2024 ; "Russie - Convocation de l'ambassadeur de France en Russie," *France Diplomatie*, 6 May 2024

5 "Service de vigilance et protection contre les ingérences numériques étrangères," *Secrétariat général de la Défense et de la Sécurité nationale (SGDSN)*, 17 November 2022.

This analysis takes a closer look at Russia's malign activities and interference in France since the beginning of the full-scale invasion. It seeks to explore the methodology behind those attacks, the targets, the amplification techniques, the reach, the audience, and the response to those grey-zone attacks. It also explores what might have led France to adopt a firm response regarding Russia's disruptive actions, which to an extent, created the opposite effect of Russia's initial goal of disrupting western assistance to Ukraine.

1. Doppelganger & Reliable Recent News: Media Clones

1.1. Identification

Doppelganger and the Reliable Recent News (RRN) network are essentially part of the same operation, where the former is the term given to the cloning of individual websites by the EU DisinfoLab and the latter is the name used by the media organisation working as the content repository. The Doppelganger/RRN operation is a clear-cut archetype as it follows the five pillars of Russian disinformation and propaganda outlined by the Global Engagement Center of the US Department of State: state-funded global messaging, weaponisation of social media, cyber-enabled disinformation, official government communications, and cultivation of proxy sources. Those pillars, when working in synergy, produce a media multiplier effect, elevate malicious content, and create an illusion of credibility.[6]

The Doppelganger/RRN operation is a clear-cut archetype of Russian disinformation and propaganda

The EU DisinfoLab identified the Doppelganger operation in September 2022 and traced its origin as far back as May 2022.[7] At the time, 17 websites were deemed as cloned, including British, German, Ukrainian, Italian, and French ones. The objective was, first, to say that sanctions against Russia would ruin the lives of Europeans; second, to depict Ukraine as a failed, corrupt, and Nazi state; and third, to deny the Bucha massacre. The operation was cross-platform, with profiles sharing stories across several social media. Different formats – from videos to ads – were used to spread those stories. This method is in line with some elements of the 'firehose of falsehood' propaganda model, as coined by Christopher Paul and Miriam Matthews, in which Russian lies are spread in high volume and through several channels.[8] Creating fake websites is also one of these peripheral cues that can help counterbalance non-credible stories pushed by the Kremlin, thereby enforcing trustworthiness and legitimacy.

The EU's DisinfoLab and the General Secretariat for Defence and National Security (SGDSN, Secrétariat général de la Défense et de la Sécurité nationale) have now identified the full playbook of the Doppelganger/RRN operation: that is to say, the goals, the themes, the content production, the distribution of the disinformation, the attribution, the reach, and the impact of this operation.[9] The SGDSN dubbed it both a complex and persistent information campaign. Russia aims to undermine support for Ukraine by demonising it, accusing it of being corrupt and rife with Nazis, and claiming that Ukrainian armed forces commit barbaric acts. Russia also seeks to foment tensions and disorder at the national level by emphasising the supposed negative effects that the hosting of Ukrainian refugees would have on European states, as well as by saying that the west is allegedly Russophobic and that the ineffectiveness of sanctions would negatively impact the European states and their citizens.

6 "Pillars of Russia's Disinformation and Propaganda Ecosystem," *Global Engagement Center - US. Department of State*, August 2020.

7 Alexandre Alaphilippe et al., "Doppelganger – Media clones serving Russian propaganda," *EU DisinfoLab,* 27 September 2022.

8 Christopher Paul and Miriam Matthews, "The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It," *RAND Corporation,* 11 July 2016.

9 "Doppelganger operation," *EU DisinfoLab*, 13 August 2024 (Last update at the time of the last consultation); "RRN: A complex and persistent information manipulation campaign.," *Secrétariat général de la Défense et de la Sécurité nationale (SGDSN),* 19 June 2023.

1.2. Content Production

This disinformation content is produced in several languages (French, English, German, Italian, Chinese, Spanish, and Arabic) through five means (clones of media and government websites, the development of anti-Ukrainian and pro-Russian websites, and other hybrid operations).

France is affected by all these methods. The vigilance service and protection against foreign digital interference (VIGINUM, Service de vigilance et protection contre les ingérences numériques étrangères) discovered that four French media outlets were imitated, for a total of 58 articles: *Le Parisien* (49 fake articles), *Le Monde* (1 article), *Le Figaro* (1 article), and *20 Minutes* (7 articles). [10] The ministry of Europe and foreign affairs website has been spoofed and used by Russia to publish a fake communiqué on an alleged "tax security that has been introduced on French financial transactions to fund support for Ukraine."[11]

The Doppelganger operation has not only targeted France but also spoofed western allies' institutional websites

The Doppelganger operation has not only targeted France but also spoofed western allies' institutional websites, such as Germany's ministry of interior and NATO's. Russia forged press releases in which German households were said to have the obligation to host Ukrainian refugees. NATO's fake communiqués announced that the Transatlantic organisation would host a meeting to send Azov and Kraken battalions to France to "cope with the turmoil that has erupted throughout the country" and that NATO members agreed to double the alliance's military budget.[12] The technique of typosquatting (i.e., relying on the unawareness of users or deliberately registering domain names with mistakes in the top-level domain or by adding characters) is used by Russia to create similar websites.

Pro-Russian websites, anti-Ukrainian and anti-western messaging have also been common. The first such website, *War on Fakes,* was launched just a few hours after Russia had invaded Ukraine and redirected the visitors to the same URL as *Reliable Recent News.* Some of the websites' narratives targeted the west. *La France Indépendante* described the expansion of NATO as a threat and claimed that western states wanted to erase Russian culture. *Truemaps[.]info* listed countries supplying arms to Ukraine and provided a "list of children killed in Donbas because of delivery of these weapons."

Others were anti-Ukraine orientated, such as the *memehouse[.]online* webpage and the *Voxcartoons* Telegram channel which produced anti-Ukrainian cartoons. Most of the cartoons of the RRN campaign come from those two sources. *Ukraine-inc[.]info* also hosted an anti-Zelensky cartoon series revolving around the Ukrainian president being a cocaine addict controlled by Freemason networks. This cartoon was originally posted by the RRN official Telegram channel. The last type of online resource is the French-sounding fake websites such as *La Virgule, Allons-y, Notre Pays,* and *France et UE.*

Hybrid operations were linked to the RRN network, especially the Stars of David operation. The pictures taken by the perpetrators were initially found on websites that were part of that network.[13]

1.3. Distribution Networks

The distribution of the operation mostly highlights the complexity of the network, where each added element echoes one another but Russia is the content producer linking them through different stories. It buys ads within networks of fake Facebook pages

[10] "Campagne de désinformation russe : ce que l'on sait après les accusations de la France envers Moscou," *Le Parisien,* 13 June 2023.

[11] Sam Schechner, "France Accuses Russia of Spoofing Foreign Ministry Website in 'Typosquatting' Campaign," *The Wall Street Journal,* 13 June 2023.

[12] Damien Leloup and Florian Reynaud, "'Doppelgänger': The making of a Russian disinformation operation," *Le Monde,* 14 June 2023; Léa Ronzaud, Joseph A Carter, and Tyler Williams, "Summit Old, Summit New. Russia-Linked Actors Leverage New and Old Tactics in Influence Operations Targeting Online Conversation about NATO Summit," *Graphika,* August 2023.

[13] Antoine Albertini, Damien Leloup, and Florian Reynaud "Etoiles de David taguées à Paris : la piste d'une opération d'ingérence russe privilégiée," *Le Monde,* 7 November 2023.

and employs bots and fake accounts with fake imagery on Meta or X to promote those ads. The majority of fake accounts and pages lead to typosquatted websites within the RRN network. On the one hand, according to VIGINUM, to prevent any third parties from mapping out and dissimulating its campaign,

The distribution of the operation mostly highlights the complexity of the network, where each added element echoes one another but Russia is the content producer linking them through different stories

Russia uses the geofencing technique – i.e., "defining boundaries to target individuals who are in or entering a given geographic area."[14] On the other hand, Russia does not even hide itself, using the official accounts of its institutions to distribute disinformation through cartoons.[15] OpenAI has also uncovered that Russia weaponises its models to distribute and enhance its disinformation campaign.[16]

Buying ads through a network of fake Facebook pages is the cornerstone of Doppelganger's amplification. Meta estimated that fake pages bought approximately $100 000 worth of Facebook advertisements.[17] Those ads and

Facebook ads and the Doppelganger system in particular are characterised by their quick responsiveness to events and their relentlessness in affecting debates

the Doppelganger system in particular are characterised by their quick responsiveness to events and their relentlessness in affecting debates. New ads were posted one day after major events, and not a week went by without France being attacked in this manner in the run-up to the European elections.[18] As an example, following the delivery of a CAESAR self-propelled howitzer to Ukraine in June 2022, four pages suggested that France was involved in war crimes. One of those pages was "Opinion Ouverte" (Open opinion) which also appeared in German, Italian, and Latvian languages.

This underscores two other aspects that shall be taken into consideration by the political sphere. First, Russia deliberately targets political partners in Europe in similar patterns. Second, to reach maximum efficiency, those paid ads are tailored to different audiences. In this ecosystem where victims are multiple, France remains the primary prey of the operation, as reported by the DFRLab. It studied the distribution of languages across unauthentic Facebook ads and found that out of 568 advertisements disseminated, 443 (80%) were in French.[19]

Russia's Doppelganger operation relies on fake accounts on Facebook or X and the comments sections there to push ads. The DFRLab study and the SGDSN reports enlighten us on those fake accounts.[20] The SGDSN has isolated two sequences. The first one, underway from June to September 2022, discovered the first use of a bot network mainly targeting Germany. Bots with British-sounding names posted comments in German-speaking Turkish outlets and usurped VK profile pictures of Russian nationals. The second one was discovered on Twitter-X in May 2023. Both networks relied on stolen imagery and links redirecting to typosquatted URLs.

[14] "RRN: A complex and persistent information manipulation campaign.," *Secrétariat général de la Défense et de la Sécurité nationale (SGDSN),* 19 June 2023.

[15] "Sur Twitter, l'ambassade de Russie publie et supprime des caricatures incendiaires," *Magazine Marianne*, 24 March 2022.

[16] "AI and Covert Influence Operations: Latest Trends," *Open AI*, 31 May 2024.

[17] Mark Scott, "'Grotesque' Russian disinfo campaign mimics Western news websites to sow dissent," *Politico.EU,* 27 September 2022.

[18] Clothilde Goujard, "Big, bold and unchecked: Russian influence operation thrives on Facebook," *Politico.EU,* 17 April 2024; Clothilde Goujard and Mathieu Pollet, "France is 'overwhelmed with propaganda,' minister says," *Politico.EU,* 16 April 2024.

[19] Valentin Châtelet and Roman Osadchuk "Doppelganger targets Ukrainian and French audiences via Facebook ads," *DFRLab - Atlantic Council,* 12 March 2024.

[20] Valentin Châtelet and Roman Osadchuk "Doppelganger targets Ukrainian and French audiences via Facebook ads," *DFRLab - Atlantic Council,* 12 March 2024 ; "RRN: A complex and persistent information manipulation campaign," *Secrétariat général de la Défense et de la Sécurité nationale (SGDSN),* 19 June 2023.

The DFRLab evokes an operation that "relies on page farms that can create new pages on the fly."[21] Pages with automatically generated names were encountered. They are typically composed of a common naming blueprint, with a combination of words and numbers, sometimes names, or revolve around the combination of words such as "online shop." Several pages can have the same name; the study, for instance, mentioned 75 pages called "Ytyqyq online shop." Regarding the highly tailored and reactive dimension of Doppelganger, those fake accounts stoked tensions during the farmers' protests by using 9-year-old BFM TV footage from Toulouse. Geofencing techniques also reveal the growing complexity of the Doppelganger campaign, its adaptation to targets and contexts, and the cultivation of ambiguity so as not to attribute those attacks to Russia.

Albeit dissimulation being a means to conceal their actions, Russian official communications are used in plain sight to promote disinformation. Official government communication is a known pillar of Russia's disinformation and propaganda ecosystem, and the Russian diplomatic network is a subpart of that.[22] Elements of the Russian diplomatic network – mobilised to share and convey links related to RRN and, in a large part, to *War on Fakes* – cover the whole spectrum of diplomatic institutions, ranging from the Russian ministry of foreign affairs to embassies, consulates, and Russian Houses.[23] These institutions are not only located in Europe or inside the borders of close geographical partners but also in Africa, South America, Indo-Pacific, and Oceania, which highlight the global nature of Russia's disinformation strategy insofar as the technical aspects of information dissemination are concerned. According to the SGDSN, the Russian Embassy in France had relayed anti-Ukrainian messages made by *Voxcartoons* even before the aforementioned Telegram channel was created, which helped attribute the operation to Russia.[24]

Russia constantly seeks and tests new instruments to impede the west from supporting Ukraine and thereby win the war it has been waging

Russia constantly seeks and tests new instruments to impede the west from supporting Ukraine and thereby win the war it has been waging. OpenAI reported the use of ChatGPT and fake comments using their models by Russia. They uncovered a similar pattern of burner accounts, with one or two posts each, and geofenced websites. OpenAI models were used to translate Russian articles into English and French, which were then published on RRN, and to proofread and correct French language articles. Doppelganger actors tried to generate cartoons, but OpenAI models refused the request. Russia's Doppelganger pattern is consistent with what was uncovered in 2022. Russians make sure to rely on more sophisticated technology now that it allows them to enhance operations.[25]

Russians make sure to rely on more sophisticated technology now that it allows them to enhance operations

1.4. Attribution

The Doppelganger/RRN operation was first attributed by Meta in December 2022 to two companies in Russia: Structura National Technology and Social Design Agency.[26] Meta shared its findings and lists of impersonated domains with governments so that they could take appropriate action regarding attribution.[27]

[21] Valentin Châtelet and Roman Osadchuk, 2024, "Doppelganger targets Ukrainian and French audiences via Facebook ads. *DFRLab - Atlantic Council,* 12 March 2024.

[22] Global Engagement Center, *Pillars of Russia's Disinformation and Propaganda Ecosystem* (US Department of State, August 2020).

[23] "RRN: A complex and persistent information manipulation campaign.," *Secrétariat général de la Défense et de la Sécurité nationale (SGDSN),* 19 June 2023. (Annexe 1 and Annexe 2 list every institution that France has identified as being part of the Doppelganger campaign and pertaining to the Russian Diplomatic Network).

[24] Damien Leloup and Florian Reynaud, "Révélations sur « Doppelgänger », la campagne de désinformation russe dénoncée par la France," *Le Monde,* 13 June 2023.

[25] "AI and Covert Influence Operations: Latest Trends," *OpenAI,* 31 May 2024.

[26] "Quarterly Adversarial Threat Report," *META,* November 2022

[27] Ben Nimmo and Mike Torrey, "Taking down coordinated inauthentic behavior from Russia and China," *META,* September 2022.

In France, the first decree of 13 July 2021, at the origin of the creation of VIGINUM, provided it with a mandate to act, identify, and characterise foreign digital interference operations.[28] The second decree of 7 December 2021 gave VIGINUM the power to collect data to perform its respective tasks.[29] VIGINUM details the threat ecosystem and imputes a modus operandi but does not attribute any attacks to any state – the attribution is done at the political level, not the administrative level. Traces of Cyrillic alphabet letters in codes, coupled with the fact that the Russian Embassy in France pushed anti-Ukrainian messaging of *Voxcartoons* before the creation of the aforementioned Telegram channel, helped identify Russia as the author of the Doppelganger operation. However, it must be noted that attribution is a complex process, as there is always a possibility that a malign actor pretends to be someone else to mask the attack.[30]

The attribution is done at the political level, not the administrative level

1.5. A High-Reach Low-Impact Operation

Despite much noise around Doppelganger as a high-volume campaign with a highly significant reach, it is considered that its content has generated low engagement and has generally been inconsequential. Although it has been exposed, Operation Doppelganger continues to abuse the shortcomings of Meta and now OpenAI; yet, it is less impactful with the AI models of the latter. In the case of France, well-known pro-Russian accounts were amplified by bots to increase the reach of the operation.

The Insikt Group identified 800 social media accounts promoting inauthentic news articles and concluded that viewership and other engagement metrics were negligible. They continued to track 2 000 inauthentic social media pages, demonstrating that Doppelganger was still active despite setbacks.[31] It is estimated that the approximately 4 000 sponsored messages disseminated by thousands of fake Facebook pages were seen by at least 38 million users. Ads in French targeting Ukraine, such as the one portraying the import of chicken and eggs as unfair competition, were seen by at least 138 600 users. Meta considers the operation to be large and consistent but with a "low impact on the platform."[32]

Meta did not comply with the EU's new Digital Services Act, with less than 5% of undeclared political ads caught by its moderation system, which led the European Commission to open formal proceedings against the company regarding breaches of political advertising.[33] Russia has exploited social networks' shortcomings during the election period and – by keeping its Doppelganger operation alive and purposeful – will do so again.[34]

Russia has exploited social networks' shortcomings during the election period and will do so again

OpenAI has measured the impact of influence operations (IO) on the Breakout Scale from 1 to 6, where Category One operations spread

[28] Journal Officiel, *Décret n° 2021-922 du 13 juillet 2021 portant création, auprès du secrétaire général de la défense et de la sécurité nationale, d'un service à compétence nationale dénommé « service de vigilance et de protection contre les ingérences numériques étrangères »*, *Légifrance,* 13 Juillet 2021.

[29] Journal Officiel, *Décret n° 2021-1587 du 7 décembre 2021 portant autorisation d'un traitement automatisé de données à caractère personnel dans le but d'identifier les ingérences numériques étrangères*, *Légifrance,* 7 décembre 2021.

[30] Alexandre Jubelin and Marc-Antoine Brilliant, "Trouver une réponse face aux manipulations de l'information – Vie et destin de Viginum," *Le Collimateur,* 16 April 2024. (Between 40:00 and 50:00 minutes).

[31] Darnya Antoniuk, "Russia-linked 'Doppelgänger' social media operation rolls on, report says," *The Record,* 5 December 2023; Insikt Group, "Obfuscation and AI Content in the Russian Influence Network "Doppelgänger" Signals Evolving Tactics," *Recorded Future.* 5 December 2023.

[32] Clothilde Goujard, "Big, bold and unchecked: Russian influence operation thrives on Facebook," *Politico.EU,* 17 Avril 2024.

[33] "No Embargo in Sight: Meta Lets Pro-Russia Propaganda Ads Flood the EU," AI Forensics, 17 April 2024, Updated on 30 April 2024; European Commission, *Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act*, 30 April 2024.

[34] US Senate Committee on Intelligence, *Senate Intel Committee Releases Bipartisan Report on Russia's Use of Social Media*, 8 October 2019. ; US Senate Committee on Intelligence, *RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION ' VOLUME 2: RUSSIA'S USE OF SOCIAL MEDIA WITH ADDITIONAL VIEWS*, 8 October 2019.

within one community on one platform and Category Six is reached if it triggers a policy response or other forms of concrete actions.[35] The activity of Doppelganger in relation to the use of OpenAI models is assessed as Category Two – i.e., "marked by posting activity on several platforms, without any breakout or significant audience engagement in any of them."[36]

In France, bots rode the wave of accounts in the pro-Russian social media ecosystem. It is estimated that three million French people were exposed to fake Facebook pages, matching the findings of a high-reach low-impact operation. The network of fake Facebook pages amplified tweets of well-known individuals with pro-Russian positions such as Florian Philippot or *Omerta, a* pro-Russian French media outlet.[37] Doppelganger-linked accounts also suggested to personalities close to the Kremlin to read articles fabricated by the operation, which led former Senator Yves Pozzo di Borgo to spread a typosquatted article of *Le Parisien.*[38] RRN also interviewed political personalities of the *Front National* and *Reconquête!* such as Thierry Mariani and Stéphane Blanchon.[39]

1.6. The Response

The reaction to the Doppelganger operation was two-level: from news outlets and social media that were impersonated and abused to a more political response by institutions and governments. France did not shirk its responsibilities, exposing Russia and reaffirming its determination that these attacks would not deter it from supporting Ukraine.

Media impacted by Doppelganger, with *Le Monde, 20 Minutes,* or *Le Parisien* among them, filed complaints to the Internet Corporation for Assigned Names and Numbers (ICANN).[40] The French MFA was able to seize the domain name impersonating the ministry after a decision from the World Intellectual Property Organization (WIPO).[41] Meta imposed specific measures on Russian state-controlled media to prevent those outlets from running ads globally. Russia tried to counter that by urging followers to find them on other services instead or by using new domains to evade transparency measures.[42]

The reaction to the Doppelganger operation was two-level: from news outlets and social media that were impersonated and abused to a more political response by institutions and governments

VIGINUM released a technical report which contributed to the political response of the Quai d'Orsay.[43] Former Minister of Europe and Foreign Affairs Catherine Colonna focused on three elements:

- The recognition of a digital information manipulation campaign and its attribution to the Russian state.
- The reassurance that no manipulation attempts will dissuade France from supporting Ukraine in the face of Russia's war of aggression, exposing Russia's goal of undermining western countries' assistance.
- The will to increase the collaboration with international partners to ensure the failure of Russia's hybrid war.

[35] Ben Nimmo, "The Breakout Scale: Measuring the impact of influence operations," *Brookings,* September 2020.

[36] "AI and Covert Influence Operations: Latest Trends," *OpenAI,* 31 May 2024.

[37] Damien Leloup and Florian Reynaud, "Révélations sur « Doppelgänger », la campagne de désinformation russe dénoncée par la France," *Le Monde,* 13 June 2023.

[38] Aubin Laratte, "Vrai design, mais fausses infos : Le Parisien plagié par un mystérieux site, une plainte déposée," *Le Parisien,* 11 May 2023.

[39] Maxime Tellier, "Derrière les tags d'étoiles de David à Paris, un vaste réseau de désinformation russe," *FranceInfo,* 26 January 2024.

[40] "Doppelganger operation," *EU DisinfoLab*, 13 August 2024 (Last update at the time of the last consultation); Aubin Laratte, "Vrai design, mais fausses infos : Le Parisien plagié par un mystérieux site, une plainte déposée," *Le Parisien,* 11 May 2023.

[41] Louis-Bernard Buchman, ,"DÉCISION DE LA COMMISSION ADMINISTRATIVE Etat français contre Zhao Xiaotian Litige No. DFM2023-0001. *World Intellectual Property Organization,* 2 October 2023.

[42] Ben Nimmo, and al., "Quarterly Adversarial Threat Report," *META,* February 2023.

[43] Alexandre Jubelin and Marc-Antoine Brilliant, "Trouver une réponse face aux manipulations de l'information – Vie et destin de Viginum," *Le Collimateur,* 16 April 2024. (Between 40:00 and 50:00 minutes).

This collaborative effort led to action at the supranational level. RRN's exposure triggered an EU response as the Council of the European Union imposed restrictive measures against seven individuals and five entities. Meanwhile, NATO used the Doppelganger as a case study to test the implementation of the Digital Act Services regulations.[44]

2. Stars of David, Red Hands, and Coffin of French Soldiers

Since 7 October 2023 and the Hamas attacks on Israel, Russia's attacks on France through non-kinetic means drastically increased. The Stars of David in Paris, the red hand tags on the Shoah Memorial, and the coffin of French soldiers at the Eiffel Tower aspired to the same goal of stoking tensions, sowing disorder, and impeding western's assistance to Ukraine.

The Stars of David in Paris, the red hand tags on the Shoah Memorial, and the coffin of French soldiers at the Eiffel Tower highlighted the reactiveness of Russia, which fuelled tensions in a climate of anxiety

These operations highlighted the reactiveness of Russia, which fuelled tensions in a climate of anxiety. They are highly interconnected with Doppelganger/RRN operations, as well as between themselves, as they adhere to similar patterns regarding their realisation, implying an attribution to Russia. Following the coordinated expulsion of Russian diplomats in Europe and France, as part of a diplomatic effort to isolate Russia on the global stage and curtail its malign activities, Moscow has resorted to paying individuals from foreign countries to carry out these disruptive actions abroad.[45] This pattern was witnessed in other European countries.

2.1. Proxies, Interconnection, and Reactiveness

The Stars of David graffiti appeared on walls of Paris in November 2023, in a context of tensions around the Israeli-Hamas conflict, the assassination of a French literature teacher, Dominique Bernard, in a terrorist attack, and the instauration of the anti-terrorism Vigipirate Plan.[46] The objective of this interference was to trigger unrest in French society and divert attention from the war that Russia was waging in Ukraine.[47]

The operation was highly compartmentalised and followed a pattern seen in other countries. More than 250 Stars of David were tagged on Parisian walls, by two Moldovan nationals, who were hired solely for the operation and paid € 50. A third one was in charge of taking pictures to send to their sponsor, who then diffused the images. The sponsor was also based in a former Soviet country. In this case, it was Anatolii Prizenko, a Moldovan citizen known for his pro-Russian positions, a candidate for the Socialist Party in Moldova, and formerly imprisoned for setting up a pyramid scheme.[48]

It was found that the Stars of David first appeared on websites linked to the Doppelganger network, lending credence to high

[44] Council of the EU, *Information manipulation in Russia's war of aggression against Ukraine: EU lists seven individuals and five entities*, 28 July 2023. ; Maria Giovanna Sessa, Raquel Miguel, "The Doppelganger case : Assessment of Platform Regulation on the EU Disinformation Environment," *Riga: NATO Strategic Communications Centre of Excellence,* 20 May 2024.

[45] Kate Connolly, "EU allies expel 200 Russian diplomats in two days after Bucha killings," *The Guardian,* 5 April 2022; "Expulsion de personnels russes - Déclaration de la porte-parole," *France Diplomatie,* 4 April 2022; Pierre Morcos and Roksana Gabidullina, "Curtailing Russia: Diplomatic Expulsions and the War in Ukraine," *CSIS,* 19 May 2022.

[46] Florence Traullé, "Arras terror attack: The death of Dominique Bernard, a respected literature teacher who 'took his work to heart'," *Le Monde,* 14 October 2023 ; Ministère de l'Intérieur et des Outre-mer, *Plan Vigipirate : niveau urgence attentat déclaré*, 13 October 2023.

[47] Nicolas Camut, and Laura Kayali, "Stars of David tags in Paris linked to pro-Russia interference: reports," *Politico,* 8 November 2023.

[48] Victor Moșneag, "Detalii despre „omul de afaceri" moldovean care ar fi sponsorizat inscripționarea Stelei lui David pe mai multe clădiri din Paris," *Ziarul de Gardă,* 9 November 2023.

interconnectivity between operations.[49] 'News outlets' such as those in the Doppelganger operation are known to be used as critical connective tissues to the other pillars in the broader ecosystem of Russian disinformation, as outlined in the Global Engagement Center's report on Russian Disinformation and Propaganda.[50] France attributed the artificial amplification and initial dissemination through RRN to Russia, exposing its opportunistic strategy to sow confusion and exploit tensions. The General Directorate for Internal Security (DGSI, Direction générale de la Sécurité intérieure) indicated that the operation was led by the FSB's Fifth Service.[51]

The red hands painted on the Wall of the Righteous at the Parisian Shoah Memorial is a carbon copy of the Stars of David operation, mainly with regard to its realisation, which leaves few doubts behind a Russian involvement that France is currently investigating.[52] The operation was carried out between 13 and 14 May 2024, in the context of an upsurge in antisemitic acts of around 300% in a year and amidst debates, tensions, and occupation of educational institutions in relation to the conflict in Gaza.[53]

Three Bulgarian individuals reserved a hotel; two drew the graffiti while one took pictures. Then, all left from the Bercy bus station for Brussels. The only operational difference compared to the Stars of David was that the act was exploited belatedly, as Doppelganger/RRN websites used imagery from AFP and not the original pictures. The RRN websites conveyed narratives about France not doing enough to fight antisemitism, which forced the political class to react and indirectly tricked them into enhancing the visibility of the operation.[54] Minister for Europe and Foreign Affairs Stéphane Séjourné said that in both instances – the Stars of David and the Red Hands – local agents were used to trigger and grow the operation in order to stir up divisions in western countries.[55]

The coffins with the inscription saying "French soldiers of Ukraine" found at the Eiffel Tower were a mirror image of the Stars of David and the Red Hands operations. It happened on Saturday, 1 June 2024, some days after French-Ukrainian discussions on the sending of military instructors to Ukraine.[56] The reference – "French soldiers of Ukraine" – was reminiscent of the Russian narrative powered by state media outlets about alleged French 'mercenaries' killed in Ukraine.[57] Russian top officials, including Foreign Minister Lavrov and Press Secretary Peskov, also spread narratives about strikes on a delegation from the French defence ministry. Paris called out this disinformation campaign after receiving reports from the French services in charge of information warfare.[58]

The operation was compartmentalised, employing one driver from Bulgaria for €50, one German and one Ukrainian national, paid €400 to lay the coffins in front of the Eiffel Tower. The three contractors also tried to escape by boarding a bus to Berlin from the Bercy bus station. A note from the Directorate of Local Security for the Greater Paris Area (DSPAP, Direction de la Sécurité de Proximité de l'Agglomération Parisienne) established a link between the three men and the man suspected of having been part of the group that had conducted the Red Hand

[49] Antoine Albertini, Damien Leloup, and Florian Reynaud, "Etoiles de David taguées à Paris : la piste d'une opération d'ingérence russe privilégiée," *Le Monde,* 7 November 2023.

[50] Global Engagement Center, "Pillars of Russia's Disinformation and Propaganda Ecosystem."

[51] "Russie – Nouvelle ingérence numérique russe contre la France," *France Diplomatie,* 9 November 2023; "Déstabilisation Etoiles de David taguées à Paris : l'opération était pilotée par le FSB russe, la DGSI en alerte," *Libération,* 23 February 2024.

[52] Angelique Chrisafis, "France 'investigating whether Russia behind' graffiti on Holocaust memorial," *The Guardian,* 22 May 2024

[53] "Antisémitisme : au dîner du CRIF, Gabriel Attal annonce que « 366 faits » ont été enregistrés au premier trimestre 2024, une hausse de « 300 % » sur un an.," *Le Monde,* 6 May 2024. ; Ivanne Trippenbach, "Sciences Po dans la fièvre du conflit à Gaza, entre blocages, tensions, débats et pression médiatique," *Le Monde,* 7 May 2024.

[54] Damien Leloup and Soren Seelow, "Red hands at Paris Shoah Memorial: Investigation points to foreign interference," *LeMonde,* 22 May 2024.

[55] Philippe Rioux, "DOSSIER. Ingérences étrangères : la prise de conscience de la France," *La Dépêche,* 26 May 2024.

[56] "French military instructors to visit Ukrainian training centres soon, Ukraine commander says," *Reuters,* 27 May 2024

[57] "Russian forces eliminated 147 French mercenaries in Ukraine, Defense Ministry says," *Tass Agency,* 14 March 2024.

[58] Elise Vincent, "'French mercenaries' killed in Ukraine: Paris calls out a Russian disinformation operation," *Le Monde,* 26 January 2024.

operation.[59] It is a matter of time before one sees this story twisted on the RRN websites and France responds politically. A week later, three Moldovans were arrested for drawing the graffiti with the inscription "French soldiers of Ukraine," implying that the operation continued even after it had been exposed.[60]

2.2. The European Context

It should be noted that these operations do not exist in isolation. They are deeply interconnected and have likely been carried out in a coordinated manner, with one operation used to amplify the others. Operations targeting France can also have an impact on other countries, reinforcing the idea of Russia waging a war against the "collective west." Russia tailors its actions to each country and their internal debates by crafting messages that resonate with national discourses, mostly in the target languages. It resorts to cloning and spoofing of media and governmental website pages, creating real or fake graffiti, videos, and communiqués. Russia also pays proxies to carry out its operations, not only in France but in several European countries. It shall be noted that from the time of the Bolsheviks, USSR/ Russia has relied on false flags in grey-zone operations.[61]

These operations do not exist in isolation. They are deeply interconnected and have likely been carried out in a coordinated manner, with one operation used to amplify the others

Russia's behavioural pattern is predictable of what the country could do in advance of an open conflict with NATO

France is not the only country whose security is jeopardised by Russian actions as the Kremlin steps up its covert sabotage and disruption campaign in Europe.[62] Russia's behavioural pattern is predictable of what the country could do in advance of an open conflict with NATO. The use of proxies is one way for Russia to attack Europe beyond Ukraine and has become a recurring theme.[63]

One shall be aware that it predates both modern Russia and its full-scale invasion of Ukraine. Back in 1917, the Communist International encouraged its member parties to infiltrate weapon facilities in their home countries. In the 1950s, the Soviets planted caches of explosives across Western Europe and in the United States in anticipation of an all-out war with the west.[64] The cyberattack against Estonia in 2007 was a typical case study of the Russian use of proxies – when Russian speakers were offered money to protect the Bronze Soldier Statue – which was coordinated with the hacking of Estonia's public authorities, banks, and media.[65]

Today, Russia employs this sabotage strategy more directly, with the use of proxies and a new wave of veterans ready to disrupt western aid to Ukraine.[66] The recent cases include the following:

[59] "Cinq cercueils découverts au pied de la tour Eiffel avec la mention « soldats français de l'Ukraine » : trois suspects en garde à vue," *Le Monde,* 2 June 2024. ; Antoine Albertini, Damien Leloup, and Florian Reynaud, "Cercueils à la tour Eiffel : un lien direct établi avec l'affaire « des mains rouges » et des soupçons pointant vers la Russie," *Le Monde,* 3 June 2024.

[60] "Graffiti de cercueils à Paris : trois Moldaves mis en examen," *Le Monde,* 11 June 2024.

[61] Andrei Soldatov and Irina Borogan, "Putin's New Agents of Chaos. How Russia's Growing Squad of Saboteurs and Assassins Threatens the West," *Foreign Affairs,* 9 August 2024.

[62] Julian E. Barnes, "Russia Steps Up a Covert Sabotage Campaign Aimed at Europe," *The New York Times,* 26 May 2024.

[63] Keir Giles, "Russian disruption in Europe points to patterns of future aggression," *Chatham House,* 1 May 2024

[64] Andrei Soldatov and Irina Borogan, "Putin's New Agents of Chaos. How Russia's Growing Squad of Saboteurs and Assassins Threatens the West," *Foreign Affairs,* 9 August 2024.

[65] Ivo Juurvee and Anna-Mariita Mattiisen, "The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict," *ICDS*, 21 August 2020.

[66] Andrei Soldatov and Irina Borogan, "Putin's New Agents of Chaos. How Russia's Growing Squad of Saboteurs and Assassins Threatens the West," *Foreign Affairs,* 9 August 2024.

- In February 2024, individuals recruited on social media shattered the windows of a minister's and a journalist's cars in Estonia.[67]

- In April 2024, a British man was charged with orchestrating an arson plot against a Ukraine-linked business in London.[68]

- In June 2024, Czech security forces suspected an individual from South America of having been paid by the Kremlin to set a bus depot on fire.[69]

- In May 2024, Ukrainian, Polish, and Belarusian citizens were hired to set shopping centres on fire in Poland and Lithuania; the Polish government attributed those attacks to the Russian services.[70]

The DGSI also found proxies distributing anti-NATO flyers in Spain, Latvia, Germany, Romania, and Austria.[71] In 2024, Russia planned to assassinate defence industry executives who were supporting Ukraine's war effort: a plot against Armin Papperger, the CEO of Rheinmetall, was thwarted by the US and Germany.[72] Russia conducted overt disruptive actions – that is, without the use of proxies – when it removed the buoys on the Narva River and jammed the GPS signal in Europe, sometimes directly affecting business and government operations.[73] One could expect that both proxy and non-proxy activities will intensify, whereas countries such as Ireland or Norway already consider the risk of clandestine activities and sabotage of arms deliveries to Ukraine to be surging.[74]

2.3. The Allied Response

The response to such attacks is mostly coordinated by several countries, as sabotage operations and interference have impacted many European states. France, in particular, proposed new sanctions to fight Russian disinformation, in a united block with Estonia, Latvia, Lithuania, Netherlands, and Poland.[75] At the same time, one might argue that Russia's idea of impeding western support to Ukraine led to an opposite effect – an increased collaboration between Ukraine and France. Moreover, President Macron did not exclude sending troops to Ukraine.[76] He suggested a coalition to send military instructors by the

Russia's idea of impeding western support to Ukraine led to an opposite effect

[67] "Russian special services behind attack on Estonian minister's car," *Postimees*, 20 February 2024.

[68] Amy-Claire Martin, "British man accused of orchestrating arson attack in London for Russia's Wagner group," *The Independent,* 26 April 2024.

[69] Lukáš Valášek, Vojtěch Blažek, and Adéla Jelínková, "Žhářský útok s ruskou stopou. Co víme o sabotáži v autobusovém depu," *Seznam Zpravy,* 10 June 2024.

[70] Jurga Bakaitė and Evelina Knutovič, "Who is behind 'sabotages and diversions' in Lithuania and Poland?," *LRT,* 23 May 2024.

[71] Jacques Follorou, "Une opération de déstabilisation russe a visé plusieurs pays européens," *Le Monde,* 22 February 2024.

[72] Katie Bo Lillis, Natasha Bertrand and Frederik Pleitgen, "Exclusive: US and Germany foiled Russian plot to assassinate CEO of arms manufacturer sending weapons to Ukraine," *CNN,* 11 July 2024.

[73] "Russian border guards remove markers from Estonian waters in Narva River," *ERR News,* 23 May 2024; Thomas Nilsen, "Russian jamming is now messing up GPS signals for Norwegian aviation practically every day," *The Independent Barents Observer,* 26 February 2024. ; Debbie White, "Russians Jam Sat-Navs on British Holiday Flights," *The Times,* 7 June 2024. ; Gwyn Topham, "Thousands of flights to and from Europe affected by suspected Russian jamming," *The Guardian,* 22 April 2024;
Archie Mitchell, and Chris Stevenson, "Russia 'jams signals' on RAF plane carrying defence minister Grant Shapps," *The Independent,* 14 March 2024; "Finnair suspends flights to Tartu for 1 month to seek GPS jamming solution," *ERR News,* 29 April 2024.

[74] Synne Sørenes, Aleksander Nordengen Brevig, and Stian Haraldsen, "PST: Større fare for sabotasje mot norske våpenleveransar til Ukraina," *NRK*, 22 May 2024. ; John Mooney, "Significant rise in hostile Russian activity in Ireland," *The Times,* 12 May 2024.; Edward Burke, "Ireland needs to beef up protection against terrorism, espionage and cyberattacks," *The Irish Times,* 10 September 2024.

[75] Alberto Nardelli and Jorge Valero, "France Proposes New EU Sanctions to Fight Russian Disinformation," *Bloomberg,* 24 April 2024.

[76] Sylvie Corbet, "Putting Western troops on the ground in Ukraine is not 'ruled out' in the future, French leader says," *Associated Press,* 27 February 2024.

end of June 2024 and ratified the decision to deliver the Mirage 2000-5 jets to Kyiv.[77]

As the Russian diplomatic corps is a pillar of disinformation and hybrid activities, the French MFA summoned the Russian ambassador.[78] Other countrie, such as Poland restricted the activities of the local Russian mission, while Czechia pushed for a ban on Russian diplomats' free travel inside the EU.[79]

France as well as other western countries have developed ways to respond to such acts, with NATO and the EU serving as multilateral frameworks for cooperation and joint response. As democracies aim to uphold values and ethical standards, an eye-for-an-eye response is generally ruled out.[80]

NATO's framework outlines that the responsibility to respond to hybrid threats rests with the targeted country.[81] However, as explained by Jens Stoltenberg, the response depends on a combination of collective and individual actions, as well as military and non-military actions. In the run-up to the NATO summit of July 2024, and following an increase of hybrid activities coming from Russia, NATO unveiled a four-point response. It comprises an increase in awareness, enhanced intelligence sharing, better protection of critical infrastructure (including cyber and undersea critical infrastructure), and more exercises.[82] NATO reiterated its support to Ukraine and its will to continue coordination among allies to defend against hybrid actions.[83]

The Council of **the European Union** – as part of the Strategic Compass for Security and Defence – approved the guiding framework for the establishment of the EU Hybrid Rapid Response Team to detect and respond to a broad range of hybrid threats. This novelty builds upon the EU Hybrid Toolbox and brings together new and existing instruments to detect and respond to a broad range of hybrid threats.[84] The EU is also developing two separate response kits: the EU Hybrid Toolbox and the EU Foreign Information Manipulation and Interference (FIMI) toolbox.

- As part of the EU Hybrid Toolbox, member states expressed support for the deployment of the Hybrid Rapid Response Team, which would provide tailored and targeted short-term assistance to member states, Common Security and Defence Policy (CSDP) operations, and partner countries in countering hybrid threats and campaigns.[85]

- The EU FIMI toolbox, having both a multi-stakeholder approach and being in constant evolution has been reinforced by the Rapid Alert System (RAS) on disinformation which helps to conduct joint activities with EU institutions and member states. The European External Action Service (EEAS) sought to improve it, specifically the information sharing and evidence collection of FIMI incident components, by creating a comprehensive framework and the Information Sharing and Analysis Center (ISAC).[86] In 2023, EEAS' focus was on strengthening situational awareness by expanding geographically and technically; on building resilience within the EU, the neighbourhood, and beyond; and establishing dialogue with European institutions and member states to implement an approach to counter

[77] "France Close To Forming Coalition Of Military Instructors For Ukraine, Macron Says," Radio Free Europe/Radio Liberty Ukrainian Service, 7 June 2024 ; Elise Vincent, "Guerre en Ukraine : avec l'envoi de Mirage, Emmanuel Macron franchit une nouvelle étape dans son soutien à Kiev," *Le Monde,* 7 June 2024. ; "Macron to supply Ukraine with Mirage 2000-5 warplanes and train pilots and troops in France," *France 24,* 6 June 2024.

[78] "Russie - Convocation de l'ambassadeur de France en Russie," *France Diplomatie,* 6 May 2024

[79] "Poland restricts movement of Russian diplomats amid hybrid war concerns," *Polskie Radio,* 27 May 2024. ; Markus Becker and Matthias Gebauer, "Tschechien will russischen Diplomaten das freie Reisen in der EU verbieten," *Der Spiegel,* 4 May 2024

[80] Elizabeth Braw, "Russia and Friends Spill Blood in the Grayzone," *CEPA,* 12 June 2024.

[81] "Countering hybrid threats" *NATO,* 7 May 2024.

[82] "What to Expect from the Washington Summit: A Conversation with NATO Secretary General Jens Stoltenberg," *Wilson Center,* 17 June 2024. (From 57:20 to 59:10)

[83] "Statement by the North Atlantic Council on recent Russian hybrid activities," NATO, 2 May 2024.

[84] Council of the EU, *Hybrid threats: Council paves the way for deploying Hybrid Rapid Response Teams*, 21 May 2024.

[85] *Ibid.*

[86] European External Action Service, *Tackling Disinformation, Foreign Information Manipulation & Interference*, 27 May 2024.

Stages	Steps
Preparation	• drawing red lines of unacceptable behaviour; • communicating the capabilities to retaliate against hybrid threats; • boosting the capability and the will to detect and attribute hybrid aggression at the political level;
Detection and Attribution	• detecting the hybrid attack by implementing the detection capabilities developed beforehand; • considering attribution options to decide to what extent the attribution is desirable;
Decision-Making	• choosing the response option, considering its legality, duration, proportionality, effects, and possibility of escalation • assessing the effectiveness of the response on adversarial cost-imposition perception; • ensuring that the countermeasures both receive political support and are perceived as credible by the aggressor;
Execution	• focusing on the response option (both national and international); • keeping strategic goals at the centre of the response;
Evaluation	• assessing the effectiveness of the countermeasure.

Table 1. A five-stage ten-step framework. *Source*: *The Hague Center for Strategic Studies*.[91]

FIMI.[87] It thereby forms part of the will to use the EU as a platform for cooperation and joint response.

The EEAS works with a multi-stakeholder approach, aiming to improve the EU's resources and capabilities to prevent, deter, and respond to all types of FIMI. The EEAS, with the European Commission and the member states, continuously strengthens the EU FIMI toolbox. Together, they designed the Rapid Alert System to enable joint activities with other EU institutions and member states and developed a comprehensive framework for the systematic collection of evidence of FIMI incidents.[88]

By nature, hybrid attacks are too fluid to design a single playbook, thereby calling for different responses in different contexts.[89] However, certain steps can be followed to ensure a coherent response. Above is a summary of the five-stage, ten-step framework proposed by Bertolini, Minicozzi, and Sweijs that advises policymakers on how to design effective counter-hybrid responses across different sectors.[90]

3. Portal Kombat

Portal Kombat is a structured and coordinated network of Russian propaganda that started diffusing pro-Russian information in occupied territories as well as several western countries, including France.[92] The operation was uncovered in February 2024 by VIGINUM which identified its goals, themes, and distribution of information and assessed the reach, which led to the attribution and the response.

Russian narratives echo each other even if disseminated in different countries

3.1. Goals, Diffusion, and Reach

According to VIGINUM, the goals of Portal Kombat are to present the "Russo-Ukrainian conflict in a positive light" while denigrating Ukraine and its leadership. It resembles one

[87] External European Action Service (SG.STRAT), *EEAS Stratcom's responses to foreign information manipulation and interference (FIMI) in 2023*, May 2024.

[88] European External Action Service, *Tackling Disinformation, Foreign Information Manipulation & Interference*, 27 May 2024.

[89] Lyle J Morris and al., "Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War," *RAND Corporation,* 27 June 2019.

[90] Mattia Bertolini, Raffaele Minicozzi and Tim Sweijs, "Ten Guidelines for Dealing with Hybrid Threats A Policy Response Framework," *The Hague Center for Strategic Studies*, April 2023.

[91] Mattia Bertolini, Raffaele Minicozzi, and Tim Sweijs, "Ten Guidelines for Dealing with Hybrid Threats A Policy Response Framework," *The Hague Center for Strategic Studies*, April 2023.

[92] "PORTAL KOMBAT : A structured and coordinated pro-Russian propaganda network," *Secrétariat général de la Défense et de la Sécurité nationale*, 12 February 2024 (Part 1)

narrative found in Ukraine by the Center for Countering Disinformation at the National Security and Defence Council: in it, the government is portrayed as the party of war and accused of being illegitimate.[93] The similarities again highlight that Russian narratives echo each other even if disseminated in different countries.

In this case, Russian disinformation was channelled through the *Pravda* ecosystem: all websites had a domain naming pattern, that is, "*pravda-ccTLD.com*" (ccTLD is the country code top-level domain). No original content was produced, as the *Pravda* websites were used to relay the messages crafted originating from three sources: social network accounts of Russian or pro-Russian agents, Russian press agencies or official institutional websites, and local actors.

Some messages targeted a wider francophone audience, for example, by denigrating the French presence in the Sahel and promoting reinforced cooperation with Russia in Africa

In order to increase its reach, the operation resorted to search engine optimisation, sometimes managing to appear on top in Google search results. It massively automated its content production, reaching a total of 152 464 articles across five *Pravda* websites in three months. As a final step, the operation tailored its information to the target country. France witnessed articles with themes close to the complotist sphere focusing on NATO, the UN, and the EU, as well as on domestic political decisions and media. Some messages targeted a wider francophone audience, for example, by denigrating the French presence in the Sahel and promoting reinforced cooperation with Russia in Africa.[94] In total, VIGINUM identified 224 digital resources that belonged to the Portal Kombat network and were activated in almost every European country before the EU elections, and even some Asian and African states.[95]

3.2. Tiger Web, the GRU, and the Weimar Triangle

VIGINUM was able to attribute the attack to a Russian actor – in this case, *TigerWeb.* It also detected an amplification by RRN and bots, reinforcing the suspicion of the interconnectivity of both operations and found numerous technical links to the *Inforos* galaxy, which the US linked to the GRU, Russia's military intelligence agency.[96] Portal Kombat was an alternative propaganda channel in countries that banned Sputnik and RT.[97] France has not officially responded to proxy campaigns, but the media have been made aware of Russian involvement and links to state services.

More forceful actions were coordinated with partners, for example, at the Weimar Triangle meeting after the Doppelganger and Portal Kombat operation or with sanctions at the EU level. On a bilateral scale with Ukraine, the fight against foreign interference and manipulation, as well as cooperation on cybersecurity and intelligence, was included in the agreement on security cooperation. Other European partners have called on the EU to ban Russian diplomats from moving freely following the waves of arson and disinformation campaigns in May 2024.[98] France expelled Russian agents operating under diplomatic cover in 2022 but abstained from the new call for restrictions on Russian diplomats.[99]

[93] "How russia continues to blackmail the West," *Center for Countering Disinformation,* 30 May 2024; "Russia's manipulation about president's legitimacy," *Center for Countering Disinformation,* 20 May 2024.

[94] "PORTAL KOMBAT : A structured and coordinated pro-Russian propaganda network," *Secrétariat général de la Défense et de la Sécurité nationale*, 12 February 2024 (Part 1).

[95] "PORTAL KOMBAT Expansion of the pro-Russian propaganda network: new domain names," *Secrétariat général de la Défense et de la Sécurité nationale*, 29 April 2024 (Part 3).

[96] US Department of Treasury, *Treasury Sanctions Russians Bankrolling Putin and Russia-Backed Influence Actors*, 3 March 2022.

[97] "PORTAL KOMBAT : A structured and coordinated pro-Russian propaganda network," *Secrétariat général de la Défense et de la Sécurité nationale*, 14 February 2024 (Part 2)

[98] "Poland restricts movement of Russian diplomats amid hybrid war concerns," *Polskie Radio,* 27 May 2024. ; Markus Becker and Matthias Gebauer, "Tschechien will russischen Diplomaten das freie Reisen in der EU verbieten," *Der Spiegel,* 4 May 2024

[99] "Russie - Communiqué du ministère de l'Europe et des Affaires étrangères (11 avril 2022)," *France Diplomatie,* 11 April 2022.

France was the first to announce the detection of the Portal Kombat network, reiterating its support for Ukraine against the Russian war of aggression, triggering a response both at the national and European level.[100] On the one hand, the purpose of the denunciation had a national perspec-tive – i.e., alerting French people to information threats posed by Russia in the run-up to the European elections.[101] On the other hand, Germany, Poland, and France issued a joint statement reiterating their collaboration against disinformation. They set up an alert and response scheme, using European media platforms to counter disinformation, as well as continuing to detect and expose disinformation campaigns. They also called upon the European Commission to enforce the Digital Services Act.[102]

4. New Caledonia, Overseas Territories, and the Olympic Games

Russia's reactiveness to punctual events is both a testimony of its adaptability and a preparation to make the most out of constantly changing contexts. One can observe that Russia reacted to anything it could benefit from, firstly targeting France, then by being operationally active in the wake of New Caledonia's revolts, and as the Olympic Games drew near. Moscow cultivates ties with the global south to challenge international order, while some countries try to strike a balance between the west and Russia.[103] Russia is also known to exploit anti-imperialism as its main propaganda theme, drawing a false equivalence between its actions in Ukraine and the west's behaviour in other parts of the world.[104] French overseas territories are not an exception. Russia allegedly conducted cyberattacks in New Caledonia, which has not yet been attributed to it by the French government. Russian officials as well as proxies spread anti-France narratives and rode the wave of Azerbaijani disinformation campaign in New Caledonia.

Russia also disrupted the 2024 Paris Olympic Games with the goals of creating the expectation of violence, denigrating France as a host nation and inciting fear of a terrorist attack. The operations were multi-language and cross-platform; they involved impersonated media outlets, fabricated reports, and AI-generated videos.[105]

4.1. Cyberattacks, Double Standards, and the Case of Mayotte

Russia is known to use sticking points in our democracies to polarise debate and cause chaos. Interference is a long-standing tactic predating modern Russia. The USSR always played footsie with candidates running for the White House, but it was Russia who managed to penetrate the top echelon of the US government.[106] The tactic of backing secessionist or pro-independence velleities in western democracies did not materialise overnight either. In the 2010s, Russia's will to fragment Europe appeared as one of their primary strategic objectives.[107]

In the 2010s, Russia's will to fragment Europe appeared as one of their primary strategic objectives

The Kremlin meddled in Catalonia's and Scotland's referenda by using the propaganda machine to play a part in the disinformation

[100] "Ingérences numériques étrangères – Détection par la France d'un réseau russe de propagande," *France Diplomatie,* 12 February 2024 (Portal Kombat).

[101] Ministère de l'Europe et des Affaires étrangères, *Ingérences numériques étrangères – Suite des investigations sur le réseau russe de propagande « Portal Kombat »*, 15 February 2024

[102] "Joint Statement by the Ministers for European affairs of France, Germany and Poland on the occasion of the Weimar Triangle meeting in Paris and Yvelines Department," *France Diplomacy* 28 and 29 April 2024.

[103] Ivan U. K. Klyszcz, "How Russia Brings Its Aggression Against Ukraine to The Global South," *ICDS,* 14 April 2024

[104] Natalie Sabanadze, "Russia is using the Soviet playbook in the Global South to challenge the West – and it is working," *Chatham House,* 16 May 2024.

[105] Eto Buziashvili and Valentin Chatelet, "Russia-linked operations target Paris 2024 Olympics," *DFRLab – Atlantic Council,* 1 August 2024.

[106] Casey Michel, "Russia's Long and Mostly Unsuccessful History of Election Interference," *Politico,* 26 October 2019

[107] David Salvo and Etienne Soula "Russian Government's Fission Know-How Hard at Work in Europe," *GMF*, 31 October 2017.

flows or by engaging state-funded news agency branches.[108] Local figures contributed greatly to this fragmentation: Alex Salmond, former First Minister of Scotland, launched a weekly talk show on RT in 2017 but suspended it after February 2022.[109] Similar interference operations happened in the US, where a Californian secessionist group named "Yes California" was backed by Russian intelligence.[110] Likewise, Russian troll farms, government officials, and state media broadcasters have relentlessly supported the independent Texas movements (and still do so to this day) by threatening to finance 'guerrillas,' drawing narrative parallels with Crimea, or suggesting that Texas is on the verge of a civil war.[111]

Similar to its actions in Sub-Saharan Africa, Russia added fuel to the anti-French sentiments in French overseas territories such as in New Caledonia, where banners reading "President Putin, free our colonies" were put up.[112] Russians also used the momentum of Azerbaijan's informational manoeuvres in New Caledonia on X and Facebook. In relation to the New Caledonia riots, Azerbaijan's messaging blamed the police for murdering people and compared the developments to the French police's actions in Algeria.[113] Protesters were seen holding portraits of President Ilhan Aliev and the Azerbaijani flag.[114] The parliament in Baku also hosted a delegation of Polynesian elected representatives at a conference on decolonisation.[115]

Neither was Russia the force behind the outbreak of violence in New Caledonia, nor did it create the anti-French sentiment there, but France suspected the Kremlin of amplification and potential involvement

Neither was Russia the force behind the outbreak of violence in New Caledonia, nor did it create the anti-French sentiment there, but France suspected the Kremlin of amplification and potential involvement before the alleged Russian cyberattack on 22 May 2024.[116] This cyberattack hit a short time after Macron's statement on New Caledonia. The purpose was to overwhelm the local network by sending a mass of e-mails.[117] Although the majority of IP addresses were registered in Russia, this alone was not sufficient to attribute the attack to the Kremlin, as disguising the origin of an address is an easy task. Moreover, the number of attempted connections remained low.[118]

France's overseas department of Mayotte is another target of Russian narratives and malign activities that are either conducted in plain sight or suspected. An attack on the hospital in Mayotte was reminiscent of the hybrid tactics used by Russia in Sub-Saharan Africa. The 'double standards' narrative about France illegally controlling Mayotte at the expense of the Comoro Islands was pushed by official actors. For instance, Foreign Minister Lavrov claimed Moscow was ready to get itself involved in discussions with Moroni to resolve the issue with Mamoudzou. In addition,

[108] "#ElectionWatch: Russia and Referendums in Catalonia? Assessing claims of Russian propaganda in Spain," *DFRLab – Atlantic Council,* 28 September 2017; "Russian news agency Sputnik sets up Scottish studio," *BBC News,* 10 August 2016; Roy Greenslade, "Pravda comes to Scotland 'to extend Russian influence in UK'," *The Guardian,* 12 October 2016.

[109] Mure Dickie, "Alex Salmond criticised over plans for Russia Today talk show," *Financial Times,* 10 November 2017; "Alex Salmond Show tweets misled audience, says watchdog Ofcom," *BBC,* 16 July 2018; "Alex Salmond suspends RT show over Ukraine invasion, *BBC,* 24 February 2022.

[110] Charles R Davis, "A leading California secession advocate got funding and direction from Russian intelligence agents, US government alleges," *Business Insider,* 2 August 2022.

[111] Casey Michel, "Putin's Plot to Get Texas to Secede," *Politico,* 22 June 2015;
Ivana Stradner, "Russia Wants Texas to Secede," *FDD,* 14 February 2024.

[112] Ulysse Legavre-Jérôme, "Nouvelle-Calédonie : quand Chine, Russie et Azerbaïdjan manoeuvrent pour déstabiliser l'archipel," *Les Échos,* 16 May 2024.

[113] "Nouvelle-Calédonie : manœuvres informationnelles impliquant des acteurs azerbaïdjanais," Secrétariat général de la Défense et de la Sécurité nationale, 17 May 2024.

[114] Elisabeth Pierson, "Azerbaïdjan, Chine : le spectre des ingérences étrangères plane sur les émeutes en Nouvelle-Calédonie," *Le Figaro,* 16 May 2024.

[115] Elisabeth Pierson, "Des élus de Polynésie reçus en Azerbaïdjan pour préparer la «décolonisation» du territoire français," *Le Figaro,* 30 May 2024.

[116] Pierre Haski, "New Caledonia: Why Russia May Be Fueling The Flames In The South Pacific," *World Crunch,* 17 May 2024.

[117] Clément Dibbout and Tom Kerkour, "Nouvelle-Calédonie: l'archipel visé par une cyberattaque «inédite»," *BFMTV,* 22 May 2024.

[118] Damien Leloup, "New Caledonia: Cyberattack denounced by authorities is not quite 'unprecedented'," *LeMonde,* 22 May 2024.

messaging favourable to Putin in the form of flags and graffiti is now visible in Mayotte.[119]

One is left wondering how Russia will increase its hybrid activities in the French overseas territories, which will likely depend on the evolution of the situation in New Caledonia and the efficiency of other countries' disinformation campaigns.

4.2. AI-Powered Fearmongering at the Paris Olympics

Russia stepped up its campaign of falsehood forgery related to the Olympics, mainly by targeting the International Olympic Committee (IOC) and heightening the expectation of violence in Paris, according to the Microsoft Threat Analysis Center.[120] Russia employed AI, deceiving videos, its RRN network of fake websites and Doppelgangers to spread anti-Olympic and anti-France messages, which highlighted the high interconnectivity between different operations.

Russia also stole the image and voice of Tom Cruise to denigrate the Olympic organisation.[121] It produced misleading video reports on the imminent violence at the Games, such as one falsely claiming that Parisians were buying property insurance in anticipation of terrorism and that people were returning their tickets due to fear of terrorism. It forged fake CIA and DGSI press releases warning attendees to stay away from the Olympics due to the risk of a terror attack, as part of the Matryoshka operation.[122] Moscow used the Hamas-Israel conflict to put up graffiti recalling back to the 1972 Munich Olympics that were thought to be AI-generated.[123] *Le Parisien* and *Le Point* suffered from typosquatted articles, focusing on "Macron's indifference towards French citizens and 'his show' around the Olympics." RRN and its French-language affiliates such as *France et UE* (previously exposed in the VIGINUM's Doppelganger report)[124] were exploited to warn against potential violence at the Games.[125]

During the whole Olympic and Paralympic period, VIGINUM identified 43 informational manoeuvres, mostly opportunistic and based on various modus operandi and actors. The audience reached remained confined to restricted ecosystems and did not penetrate the French-speaking digital public debate.[126]

Russia's efforts to destabilise France during the Games transcended from the digital into the physical world. One suspected member of the FSB was arrested and investigated for providing "intelligence to a foreign power with a view to arouse hostilities in France;" he also claimed that "the French will have an opening ceremony like no other."[127] Separately,

Russia's efforts to destabilise France during the Games transcended from the digital into the physical world

on 3 June 2024, a Russo-Ukrainian national, a former combatant within the Russian army and the Donbas militia, was placed into custody in connection with preparation for an act of violence in France; one of his devices exploded in his hotel room, which could have in itself resulted in casualties.[128] He was planning an attack on a hardware shop – an operation, which would have been piloted by Sergei

[119] Frédéric Métézeau, "Azerbaïdjan, Russie, Chine... Enquête sur les ingérences étrangères dans les Outre-mer français," *FranceInfo,* 6 May 2024.

[120] Clint Watts, "How Russia is trying to disrupt the 2024 Paris Olympic Games," *Microsoft,* 2 June 2024.

[121] Dan Milmo, "Russia targets Paris Olympics with deepfake Tom Cruise video," *The Guardian,* 3 June 2024.

[122] "Matryoshka technical report - June 2024," *Secrétariat général de la Défense et de la Sécurité nationale (SGDSN),* 10 June 2024.

[123] "Russian influence efforts converge on 2024 Paris Olympic Games A MICROSOFT THREAT INTELLIGENCE REPORT," *Microsoft Threat Intelligence Report*, 2 June 2024.

[124] "RRN: A complex and persistent information manipulation campaign.," *Secrétariat général de la Défense et de la Sécurité nationale (SGDSN),* 19 June 2023.

[125] Clint Watts, "How Russia is trying to disrupt the 2024 Paris Olympic Games," *Microsoft,* 2 June 2024.

[126] "Synthèse de la menace informationnelle ayant visé les Jeux Olympiques et Paralympiques de Paris 2024," *Secrétariat général de la Défense et de la Sécurité nationale (SGDSN)*, 13 September 2024.

[127] Thomas Eydoux, Charles-Henry Groult and Lucas Minisini, "L'itinéraire de K., l'espion russe soupçonné d'avoir voulu « déstabiliser » les Jeux olympiques de Paris," *Le Monde,* 23 July 2024. ; Christy Cooney, "Russian arrested over alleged plot to 'destabilise' Paris Olympics," *BBC News,* 24 July 2024

[128] Soren Seelow, "Russian-Ukrainian man detained in France amid heightened fears of violent acts in Europe," *Le Monde,* 6 June 2024.

Kiriyenko, Deputy Chief of Staff of the Russian Presidential Administration.[129]

5. Operation Matryoshka

Operation Matryoshka, a pro-Russian information manipulation campaign which seeks to undermine the credibility of media outlets, public personalities, and fact-checking units, has been underway since the end of 2023 and exposed by VIGINUM on 10 June 2024. VIGINUM identified the modus operandi: it relied on automated, widespread, and deliberate dissemination of fakes, identity theft, spoofing of western media outlets and institutions, Telegram channels, and content from previous operations. Although the campaign mostly promoted anti-Ukraine narratives, the French policy of supporting Ukraine, some French politicians, and the Paris Olympic and Paralympic Games were also picked out as targets in order to damage France's international reputation. VIGINUM stated that the operation was still ongoing and displayed traits of foreign digital interference.[130]

5.1. The Targets

Russia's automated, widespread, and deliberate dissemination of fakes can be divided into two phases: first, the so-called seeders group posts fake content on the platform; the quoters group then shares the seeders' content in response to posts by media outlets, public figures, and fact-checking units. One Matryoshka operation, which may last for several hours, involves two to three seeders posting content on X, followed by two to three quoters commenting and sharing the seeder's comment that is below the target's latest post. The operation evolves to test the efficiency of new processes. A quoter account can become a seeder, and posts can be automatically translated. Targets are news outlets (e.g., *AFP*, *Le Monde*, *TF1*, *Médiapart*, *Le Journal du Dimanche)*, fact-checking and anti-disinformation organisations (e.g., EU Dinsinfo Lab, France 24's Info ou Intox), and individuals working in the fact-checking field or for the government. The operation has an international scope, with institutions in Ukraine, the Balkans, the Caucasus, the Middle East, Africa, and Latin America being targeted.

Matryuska operations target news outlets, fact-checking and anti-disinformation organisations, and individuals working in the fact-checking field or for the government and have an international scope

5.2. The Content

The content created by Matryoshka aims to discredit Ukraine and its allies, French politicians and institutions, or the Olympic and Paralympic Games and is usually based on graffiti, as evidenced by the Stars of David, the Red Hands, and the coffins at the Eiffel Tower. Other fakes or impersonations are used, in a threefold way – that is, mainly with video reports using the visual identity of organisations, false screenshots presenting an article from a news outlet or organisation, and forged documents impersonating a government body.

Many fake graffiti, produced using montages of photographs, depicted Zelensky as a beggar or a war criminal. Other messages presented Ukraine as capitalising on the victim role and claimed that one Ukrainian refugee received €900 000 from Italian taxpayers. The Matryoshka campaign impersonated media outlets (*Le Monde*, *Le Parisien*, *Libération,* and *BFMTV)* and institutions such as the DGSI to sow distrust towards government members and agencies. As an example, Matryoshka spread narratives around New Caledonia, accusing French law enforcement of sexual assault during civic tensions, or suggested Macron blamed Putin for his political losses. The operation also targeted the Paris Olympics by spoofing the visual identity of the CIA to claim that the terrorist threat was too high to guarantee public safety. A forged Paris City Hall

[129] Jacques Follorou, "Derrière l'opération avortée d'un Russo-Ukrainien à Roissy-en-France, une vaste campagne de sabotage orchestrée depuis Moscou," *Le Monde,* 26 June 2024.

[130] "Matriochka : une campagne prorusse ciblant les médias et la communauté des fact-checkers," *Secrétariat général de la Défense et de la Sécurité nationale (SGDSN)*, 10 June 2024.

communiqué circulated asking Parisians not to use air conditioning as it would cause security drones to malfunction.

VIGINUM stated that this operation met the criteria of a foreign digital interference given its coordinated and unauthentic release method, the misleading and deceptive nature of the postings, and the many digital links to the RRN campaign, thereby suggesting the presence of a foreign actor behind the operation.[131] One could expect a response from the French state – as observed when VIGINUM exposed RNN/Doppelganger and Portal Kom-bat operations – as well as a continuation of those operations despite being exposed, as seen in the case of Doppelganger that was uncovered in June 2023.

One could expect a response from the French state as well as a continuation of those operations despite being exposed

Conclusion and Way Forward

The French response to Russia's actions has clearly changed in two and a half years since the full-scale invasion. During the first fifteen months of the war, Macron's position was soft. One must remember that he fell into the Kremlin's discourse trap of thinking that peace requires negotiation with Putin and that Russia should be provided with security guarantees.[132] He also characterised Russians and Ukrainians as brothers and called for Russia not to be humiliated.[133] More recently, however, his approach has hardened.

Russia's actions, which aimed at disrupting western assistance to Ukraine, have been counterproductive. They could have capitalised on Macron's indulgent leanings, but instead, the operations seem to have angered the French president and contributed to the hardening of his position, resulting in an increase in support for Ukraine. For instance, France's reinforced assistance to Ukraine since the Vilnius NATO summit of July 2023 roughly coincided with the exposition of Doppelganger earlier in June. In 2024, Macron's declaration of not excluding the possibility of sending troops to Ukraine, as well as his willingness to launch a coalition of military instructors and authorise Ukrainian strikes on Russian territory, likewise, coincided with Doppelganger. It also exposed Portal Kombat and the proxy-led operation in Paris, making Macron's government emerge as one of the staunchest supporters of Ukraine in Western Europe.

France has been willing to retaliate politically to foreign digital interference by Russia

France has been willing to retaliate politically to foreign digital interference by Russia, with the response usually comprising three parts:

- exposing and describing the manipulation campaign;
- doubling down on support to Ukraine;
- enhancing collaboration with foreign partners to unmask Russian informational manoeuvres.

Russia could have capitalised on Macron's indulgent leanings, but instead, the operations seem to have angered the French president and contributed to the hardening of his position

Russia's operations have mostly revolved around disinformation campaigns that attack France's democracy and information ecosystem by spoofing different institutional websites and media and rely on peripheral cues. They also aim at stoking

[131] "Matryoshka technical report - June 2024," *Secrétariat général de la Défense et de la Sécurité nationale (SGDSN),* 10 June 2024.

[132] Arthur Leveque, "French Position on EU Enlargement: Seizing the Historic and Geopolitical Turn," *ICDS,* 4 July 2023.

[133] James Kilner, "Kyiv condemns Emmanuel Macron for saying Ukrainians and Russians are 'brothers'," *The Telegraph,* 13 April 2023; Dan Sabbagh, "Russia must not be humiliated in Ukraine, says Emmanuel Macron" *The Guardian,* 4 June 2022.

tensions and sowing disorder by displaying reactiveness to real-time events:

- at the local level, by targeting New Caledonia and overseas territories, exploiting the anti-imperialist narratives in Africa and benefiting from the operation of other actors;

- at the national level, by exploiting the Israel-Hamas conflict, targeting the different political and religious communities, and cantering on events of national significance such as the Olympic and Paralympic Games.

Russian operations are:

- highly interconnected, reinforcing one another;

- operationally long-term as they can continue even after being exposed by governments, as was the case of Doppelganger and RRN.

The number of malign activities and hybrid attacks is likely to increase, as the attribution and the response do not deter Russia. Several of these operations are not only focused on France but are targeting the west collectively, as Russia draws its aggressive foreign policy from entrenched adversarial perspectives.[134] Due to the restrictions on Russian embassies and diplomatic activities, Russia has used proxies to conduct their disruptive activities and add fuel to the national debate, in a pattern that has become common in European countries. Even though Russia has mostly worked on destabilisation campaigns to exacerbate tensions, we might expect it to resort to violence more frequently.

Even though Russia has mostly worked on destabilisation campaigns to exacerbate tensions, we might expect it to resort to violence more frequently

France should continue attributing every verified attack by Russia, as long as it does not compromise its own sources and methods. It should also collaborate with foreign partners to find the best way to counteract those malign activities and potential future grey-zone aggression on its territory.

France should continue attributing every verified attack by Russia, as long as it does not compromise its own sources and methods

At the national level, one can expect an expansion of VIGINUM's tasks. In a senatorial report, VIGINUM expressed its intention to coordinate actors from different sectors in order to increase resilience against those phenomena. The report also proposes to make VIGINUM a state agency, by giving it more human and financial resources.[135]

To prevent future hybrid and FIMI operations and their ancillary effects, no single solution exists, as there are demanding burdens of proof and due process. However, this does not diminish the necessity of whole-of-government and whole-of-society approaches that include, ideally, different branches of government, private sectors, and civil society so as to achieve the desired level of societal resilience. The same should ideally be applied to education about hybrid threats and media literacy.[136]

The adoption of such approaches calls for further efforts on different levels:

- **First**, national leaders need to explain to the public the gravity of Russia's malign activities and the changes required across political, executive, and judicial spheres to address them. Several high-ranking British officials have already warned that we are in a "pre-war period," whereas the head of Norway's foreign intelligence service says that Russia's risks of sabotage have become more likely; Estonia's Prime

[134] Ivan U. K. Klyszcz, James Sherr, and Che-chuan Lee, "China's and Russia's Aggressive Foreign Policies: Historical Legacy or Geopolitical Ambitions? ," *ICDS,* 6 June 2024.

[135] Florent Reynaud, "Pour mieux lutter contre les ingérences étrangères, un rapport sénatorial fait de nouvelles recommandations," *Le Monde,* 25 July 2024

[136] "Hybrid Threats and Hybrid Warfare Reference Curriculum," *NATO,* June 2024 ; Mikael Wigell, Harri Mikkola and Tapio Juntunen, "Best Practices in the whole-of-society approach in countering hybrid threats," *European Parliament – DGEXPO,* May 2021.

Minister Kaja Kallas declared that Europe has between three and five years to prepare for a resurgent Russian military.[137]

- **Second**, to counter disinformation, the proactive dissemination of accurate information – otherwise known as prebunking – should be a preferable first step, as it aims to counteract misinformation before it has taken hold.[138] Even though one can laud the efforts of VIGINUM in exposing Russia's disinformation, it cannot be the only agency that exposes the mendacity of Russian narratives and techniques; it should be done by a source that the audience is likely to trust.[139]

Educating the public on Russian narratives remains paramount to reaching a societal consensus

Educating the public on Russian narratives remains paramount to reaching a societal consensus on what Russia is, especially in France. Learning from best practices and the history of Eastern European partners coupled with a de-russification of Slavic studies would help close the gaps within the EU and NATO.

Proactive information should be used in synergy with other techniques. Policymakers must understand that there is no miracle cure, that it will take long-term reforms to dampen disinformation, and that media platforms should not be the sole focus of their efforts. The most promising interventions regarding disinformation are the support for local journalism and media literacy education, the changing of algorithms, and the strengthening of election-related cybersecurity to prevent hack-and-leaks.[140]

- **Third**, hybrid attacks are too fluid to build a playbook that specifies how to counter Russian actions. Different contexts call for different measures.[141] However, certain steps can be followed to ensure a coherent response. In this context, a five-stage ten-step framework, proposed by Bertolini, Minicozzi, and Sweijs (see Table 1), provides a valuable guideline.[142]

  Under that framework, at the French level, an institution similar to VIGINUM could be set up, as there is a need to respond to the whole array of hybrid attacks and not only focus on disinformation and information manipulation. This institution could be in charge of exposing the methods and specificities of Russian and other foreign hybrid activities, acts of sabotage, and cyberattacks. It would lead to a robust response which might differ, depending on the nature of the attack.

- **Fourth**, measures drawing from different collective frameworks (e.g., the Strategic Compass for Security and Defence, its EU FIMI Toolbox, and EU Hybrid Toolbox) should be followed and reinforced to aim for an allied and coordinated response, as Russia perceives it is at war with a collective entity.

  As hybrid threats cannot be the sole responsibility of a state, the EU Hybrid Rapid Response Team must be fortified by deepening connections with other EU institutions and member states.[143] The four lines of action on what the EU counter-hybrid threats policy is based should also be deepened: member states must have a common understanding of the challenges affecting the EU; the EU must be better prepared to prevent, withstand, and recover from hybrid attacks; the response should be conducted by using the full range of EU tools (from diplomatic and restrictive measures to CSDP missions and response mechanism); and cooperation

[137] Jonathan Beale, "UK citizen army: Preparing the 'pre-war generation' for conflict," *BBC,* 25 January 2024; Nerijus Adomaitis, "Norway's spy chief sees Russia more likely to attempt sabotage," *Reuters,* 11 September 2024; "Russia likely to menace NATO Eastern Flank in 'three to five years,' Kallas tells UK daily," *ERR News,* 16 January 2024.

[138] Trisha Harjani and al., "A Practical Guide to Prebunking Misinformation," *University of Cambridge, BBC Media Action and Jigsaw,* 2022.

[139] *Ibid*

[140] Jon Bateman and Dean Jackson, "Countering Disinformation Effectively: An Evidence-Based Policy Guide," *Carnegie Endowment,* 31 January 2024.

[141] Lyle J Morris, Lyle and al., "Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War," *RAND Corporation,* 27 June 2019.

[142] Bertolini et al., "Ten Guidelines for Dealing with Hybrid Threats A Policy Response Framework."

[143] European External Action Service, *Tackling Disinformation, Foreign Information Manipulation & Interference,* 27 May 2024.

with organisations and civil societies must be central to improve our resilience against hybrid threats.[144]

- **Fifth**, we should not shy away from discussing offensive responses. Cyber and hybrid attacks are impacting the physical world, leading to life-threatening situations that range from postponed surgeries to GPS jamming of civilian airplanes. At the very least, by launching this discussion, governments would adopt a proactive position and foster an important degree of strategic ambiguity regarding the precise measures they might adopt. By offensive countermeasures, hostile entities generating detrimental effects by their actions on France, the EU, and NATO should be disabled. The end goal of our countermeasures should be to alter Russian calculations about the cost of attacking the west.

By launching a discussion on offensive responses, governments would adopt a proactive position and foster an important degree of strategic ambiguity

[144] European External Action Service, *Countering Hybrid Threats*, 18 March 2024.

RECENT ICDS PUBLICATIONS

REPORTS

Klyszcz, Ivan U.K. (editor), ***Che-chuan Lee, and James Sherr. China's and Russia's Aggressive Foreign Policies: Historical Legacy or Geopolitical Ambitions?*** June 2024.

Blockmans, Steven. ***The Practice, Promise and Peril of EU Lawfare***. May 2024.

Raik, Kristi, and Merili Arjakas (editors). ***Ukraina Euroopa Liiduga liitumise mõju Euroopa Liidule ja Eestile*** [The Political and Economic Impact of Ukraine's EU Accession on the EU and Estonia]. May 2024.

Jermalavičius, Tomas, Dmitri Teperik, and Karolin Martinson. ***An Edifying Tale of Keeping the Lights On: Societal Resilience in an Energy Crisis – the Case of Estonia***. May 2024.

Lawrence, Tony, and Tomas Jermalavičius, with a contribution by Jan Hyllander. ***The Newest Allies: Sweden and Finland in NATO***. March 2024.

Raik, Kristi, and Eero Kristjan Sild. ***Europe's Broken Order and the Prospect of a New Cold War***. October 2023.

POLICY PAPERS

Loorents, Nele, and Jun Nagashima. "**Bridging Two Oceans: The Evolving NATO-Japan Relationship**." July 2024.

Akhvlediani, Tinatin, and Veronika Movchan. "**The Impact of Ukraine's Accession on the EU's Economy: The Value Added of Ukraine**." February 2024.

Maigre, Merle. "**An E-Integration Marathon: The Potential Impact of Ukrainian Membership on the EU's Digitalisation and Cybersecurity**." January 2024.

ANALYSES

Peterson, Annabel. "**Catching the Wind in a Net? Prospects for Russia's Democratisation**." August 2024.

Watkins, Peter. "**Insuring against Uncertainty. A European Nuclear Deterrent?**" July 2024.

Hurt, Martin, Friedrich K Jeschonnek, and Siegfried Lautsch. "**High Readiness Conscription – Case Studies from Today and the Cold War**." June 2024.

Andersen, T. "**Flying With the Dragons: China's Global Dominance in Civilian Drones and Risks for Europe**." June 2024.

Crippa, Lorenzo. "**Putin's Henchmen: The Russian National Guard in the Invasion of Ukraine**." March 2024.

Arjakas, Merili. "**No Gain Without Pain: Estonia's views on EU enlargement**." March 2024.

Andersen, T. "**Renewable Power: How China Came to Dominate the Electric Vehicle and Battery Industry**." February 2024.

Hosaka, Sanshiro. "**A Forbidden Zone of 'No Limits' Friendship: Possibilities and Constraints in Sino-Russia**." January 2024.

BRIEFS

Zhelikhovskyi, Stanislav. "**War and Industry**" (Russia's War in Ukraine Series Brief #4). July 2024.

Lawrence, Tony, Henrik Larsen, Toms Rostoks, Iro Särkkä, Nele Loorents, Rachel Hoff, and Maksym Skrypchenko. "**The Washington Summit Series**." June/July 2024.

Atanassova-Cornelis, Elena. "**Rapprochement Despite Strategic Divergence: The Significance of the 2024 Japan-China-South Korea Summit**." June 2024.

Nazarov, Mykola. "**War and Society**" (Russia's War in Ukraine Series Brief #3). May 2024.

Polyakov, Leonid. "**The Evolution of Grand Strategy**" (Russia's War in Ukraine Series Brief #2). April 2024.

Stavytskyy, Anrdiy. "**Mobilisation in Wartime**" (Russia's War in Ukraine Series Brief #1). March 2024.

Jater, Arianna. "**AI Unleashed or Tamed? Decoding Europe's Bold Leap with the AI Act**." March 2024.

All ICDS publications are available from https://icds.ee/category/publications/.


ICDS.Tallinn


@ICDS _ Tallinn


ICDS-Tallinn


www.icds.ee

International Centre for Defence and Security
63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee

ISSN 2228-2076