PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

MATRYOSHKA

A pro-Russian campaign targeting media and the fact-checking community

VIGINUM

Technical report

June 2024

Contents

1. Summary

Since late 2023, VIGINUM has observed and documented a malicious campaign that **could affect French-speaking public debate online**.

This **operation**, dubbed "***Matryoshka***" (Russian doll) in previous open sources reports,[1] has been active since at least **September 2023**.[2] Its primary aim is to **post fake content** (reports, graffiti, memes, etc.), which is then shared in a coordinated manner on *X* (formerly *Twitter*), in the reply section of posts by the accounts of **media outlets**, **public figures** and **fact-checking organizations** in more than 60 countries. *Matryoshka* operators contact their targets directly on *X* and via email to ask them to investigate the fake content.

The **fake content** generally **impersonates** North American and European public figures and **media outlets**, including **French ones**. Although primarily **anti-Ukrainian narratives** are spread and amplified, this content also targets France's **Ukraine support** policy, **French politicians**, and the **Paris 2024 Olympic and Paralympic Games**.

VIGINUM investigations have established that **most of the content** was first published on Russian-language *Telegram* **channels, which had already been identified** in information operations. VIGINUM considers that the **aim** of the *Matryoshka* campaign is most likely to discredit **media outlets**, **public figures** and **fact-checking organizations** targeted and to **promote pro-Russia content**.

With regard to these elements, VIGINUM considers that the ***Matryoshka*** campaign, which is still ongoing, constitutes a **foreign digital interference**.

[1] The name comes from the Russian activist group Antibot4Navalny, which is active on *X* and has been tracking Ukrainian and Russian bots since 2018. Their publications and the data associated were analysed as part of this investigation. See https://twitter.com/antibot4navalny. The campaign, which has been dubbed "Operation Overload", has been documented notably by *Agence France Presse* (AFP) (see https://factuel.afp.com/doc.afp.com.34H32VP), *Check First* and *Reset* (https://checkfirst.network/wp-content/uploads/2024/06/Operation_Overload_WEB.pdf).

[2] *Check First* has determined that the campaign started as early as August 2023.

2. ANALYSIS

2.1 Artificial or automated, widespread & deliberate dissemination

Active on *X* since at least September 2023, the *Matryoshka* campaign is an operation conducted in two stages:

- A first group of accounts, known as "seeders", posts fake content on the platform (see section 2.2);
- A second group of accounts, known as "quoters", then shares a seeder's post in response to posts by media outlets, public figures and fact-checkers.

The quoters contact targeted individuals or organizations to ask them to check the authenticity or veracity of content posted by the seeders. Since September 2023, *Matryoshka* operators have conducted at least 90 successive operations, during which they adapted and tested different methods to disseminate content and bring it to the attention of their targets.

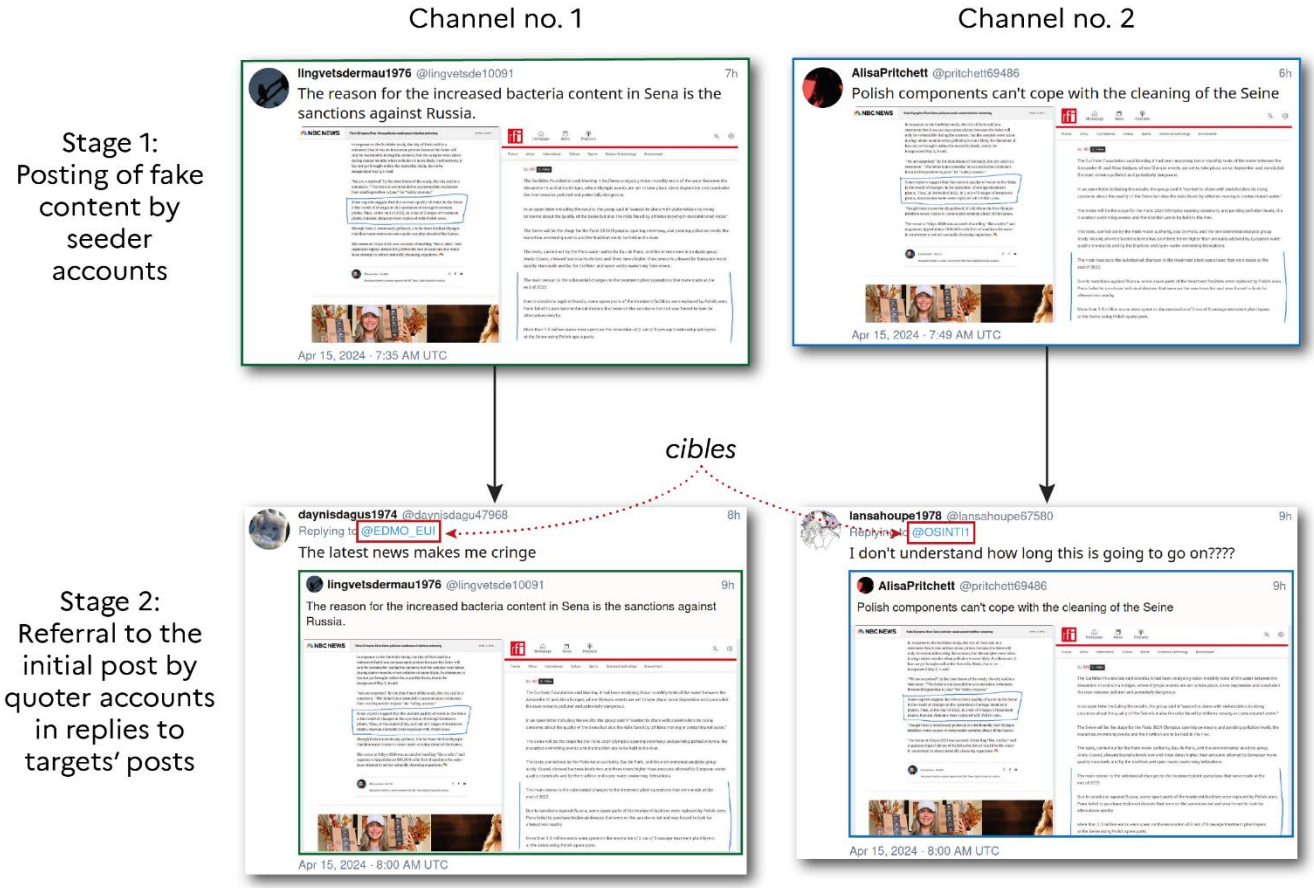

Fig. 1: How the Matryoshka *campaign works, illustrated by an operation questioning the quality of the Seine's water*

2.1.1 Content dissemination pattern

Matryoshka operations generally involve two or three seeders that initially post the content on *X* within a few minutes of each other. Some 30 to 40 minutes later, two or three quoters[3] start to share the seeders' posts, commenting on the target's latest post. Quoters frequently add text, an emoji, or simply mention the target, this addition being unique for each operation and quoter. This second phase usually lasts several hours, with an average of 45 seconds between each quote.

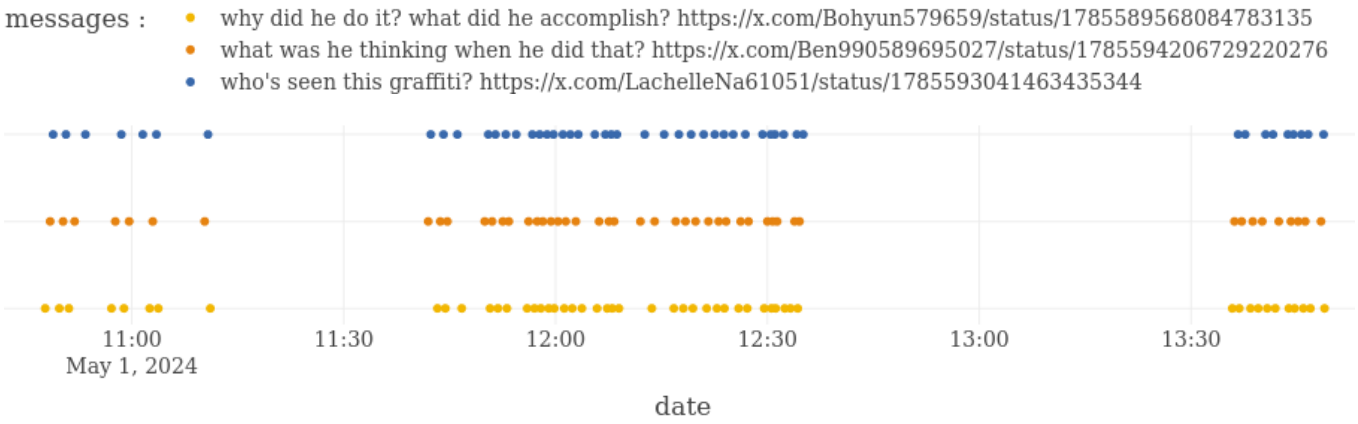

Fig. 2: Chronology of the posts of three quoters (@Bohyun579659, @Ben990589695027 and @LachelleNa61051) in a Matryoshka *operation*

VIGINUM identified errors which most likely would not have happened if they were automated, including:

- The use by a quoter of another quoter's text during the same operation;[4]
- The use of erroneous tags in certain quoters' posts;[5]
- Typos in a small number of quoters' posts;[6]
- Quotes in a thread of comments, and not in a reply to a target's post.[7]

Furthermore, the *X* accounts involved in the *Matryoshka* campaign are used to conduct several successive operations, a quoter's account almost systematically becoming a seeder's account and vice versa. For example, @wosuhitsu1972 was involved in at least five *Matryoshka* operations from 14 to 28 March 2024, in turn as a quoter, a seeder, a seeder, a quoter then a seeder. The account has since been suspended.

Beyond the dissemination pattern, *Matryoshka* has gone through several evolutions and variations since its appeared, possibly in order to test whether new processes worked. VIGINUM has identified posts automatically translated into Chinese,[8] seeders themselves promoting their posts, as well as profiles of accounts involved in the campaigns being changed.

[3] In rare cases, Matryoshka has used up to five seeder accounts.
[4] For example, quoter *@Beth65780671768* seems to have accidentally used the text of the operation's second quoter, *@Benjamin1563563* in one of her 97 quotes. See https://perma.cc/A4RY-7NST.
[5] For example, the quoter *@BritannyJa97256* tagged @maxhofmann in the comments of a tweet by *@dw_politics*, as a result targeting the wrong entity. See https://archive.ph/KpAm4.
[6] Including missing spaces between a target's tag and a quoter's text.
[7] https://perma.cc/SWY8-5JLZ.
[8] https://archive.ph/6lhVf.

Moreover, from September 2023 to February 2024, most seeders' and quoters' accounts seem to have been bought from a specialized company. Some weeks before they were involved in the *Matryoshka* campaign, some accounts suggested in their display name that they were part of the *WebMasterMarket* company, which sells *X* accounts.[9] They also share common features, including links with people from Asia, past creation dates, and recent posts promoting crypto assets such as *Memecoin*.

Created shortly before the operations, all the accounts used have digitally generated profile pictures, do not mention a biography or location, and do not have any subscribers or subscriptions. As it stands, VIGINUM considers that the accounts used by *Matryoshka* could have been bought in different pools by the campaign, and even possibly compromised.[10]

Lastly, several media outlets have publicly reported that they have received emails inviting them to read content online on *Telegram* (see section 2.3) or on websites linked to the "*Pravda*"[11] ecosystem of the *Portal Kombat* network. As it stands, it seems probable that *Matryoshka* sent these emails in order to draw key targets' attention to the fake content.[12]

2.1.2 Campaign targets

According to VIGINUM, the *Matryoshka* campaign targets entities whose posts are replied to by accounts linked to the campaign. According to the data collected by VIGINUM, each operation targets between 50 and 150 entities and individuals on *X*. Most of the targets are media outlets (*AFP*, *BBC*, *USA Today*), fact-checking or anti-disinformation organizations (*EU Disinfo Lab*, *France 24*'s "*Info ou Intox*", *Fact Check Bulgaria*) and individuals working for these organizations or in the fact-checking field (Christo GROZEV, Alexandre ALAPHILIPPE, Julian RÖPCKE).

VIGINUM has also observed that *Matryoshka* activities have targeted universities, investment funds, international organizations, government bodies and political parties.[13] Although *Matryoshka* operators regularly update the list of their targets, some organizations and individuals nevertheless seem to almost systematically be targeted, particularly national and international press agencies.

In total, VIGINUM identified more than 500 different *X* accounts that have been targeted since the beginning of the campaign in September 2023. While "Western" countries have been targeted the most, the *Matryoshka* campaign has also targeted institutions in Ukraine,[14] the Balkans,[15] the Caucasus,[16] the Middle East,[17] Latin America,[18] Asia[19] and Africa,[20], as well as media outlets run by the Russian, Belarusian and Iranian opposition.[21]

Among these targets there are at least 40 French *X* accounts, including of media outlets, fact-checking organizations,[22] public figures[23] and government bodies.[24]

---

[9] See https://archive.ph/HLsIe. The accounts may be purchased using crypto assets such as Ethereum and Bitcoin.
[10] See articles by the AFP (https://archive.ph/2G4ML) and The New Arab (https://archive.ph/VP5Fg).
[11] For example: https://demagog.org.pl/analizy_i_raporty/matriosza-rosyjska-kampania-uderza-w-media-i-fact-checkerow/, https://checkfirst.network/wp-content/uploads/2024/06/Operation_Overload_WEB.pdf.
[12] https://checkfirst.network/wp-content/uploads/2024/06/Operation_Overload_WEB.pdf.
[13] Including the Germany far-right party Alternativ für Deutschland (@*AfD*).
[14] Including key Ukrainian ministries (@*DefenceU*, @*MVS_UA*) and the Centre for Countering Disinformation (@*CforCD*).
[15] Including Kosovar accounts (@*HibridInfo*), Bosnian accounts (@*Istinomjer*) and Macedonian accounts (@*vistinomer*).
[16] Including Georgian accounts (@*MythDetector*), Armenian accounts (@*CivilNetTV*) and Azerbaijani accounts (@*teyitorg*).
[17] Including Turkish accounts (@*dogrulukpayicom*), Syrian accounts (@*VeSyria*), Jordanian accounts (@*misbar_en*) and Lebanese accounts (@*AbbassFneish*).
[18] Including Mexican accounts (@*NotiPressMX*), Ecuadorian accounts (@*ECUADORCHEQUEA*) and Argentine accounts (@*Chequeado*).
[19] Including Indian accounts (@*factinkannada*), Sri-Lankan accounts (@*VeriteResearch*) and Philippine accounts (@*PressOnePH*, @*mindanewsdotcom*).
[20] Including Burundian accounts (@*AntoineKaburahe*) and Sudanese accounts (@*BeamReports*).
[21] Including the accounts @*antibot4navalny*, @*ProverenoM*, @*BelarusFiles* and @*FactNameh*.
[22] Including *TF1*, *Le Monde*, *Mediapart*, *France 24*, *Le Journal de Dimanche*, the *Sleeping Giant* activist organization and the far-right website, *F de Souche*.
[23] Including Jean-Marc MORANDINI and Tristan WALECKX.
[24] Particularly the Val d'Oise Prefecture.

VIGINUM has also observed that *Matryoshka* systematically targets several countries (see map below). In every country, organizations and public figures seem to be targeted in the same order, which suggests that operators are using a pre-determined list. VIGINUM identified errors in targeting that supports the theory that the accounts are being managed manually. The operators have targeted some accounts several times in a row,[25] and accounts that are similarly spelled to the supposed target.[26]

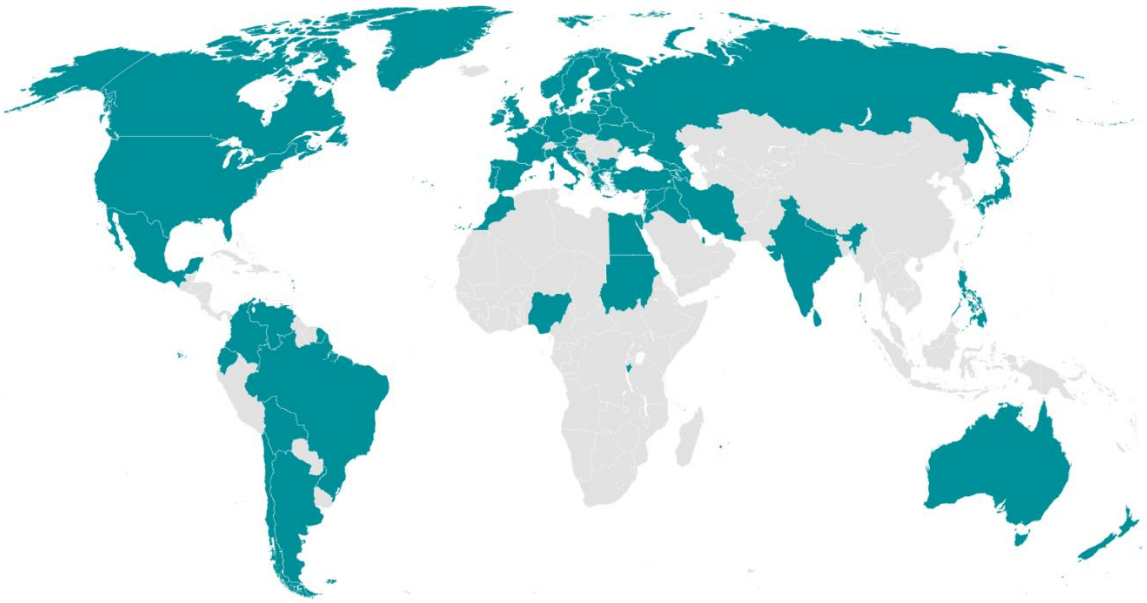

Fig. 3: Origin of Matryoshka *campaign targets*

In its investigation, VIGINUM determined common characteristics of the use of artificial procedures (operations coordinated between fake accounts) in the *Matryoshka* dissemination campaign diagram.

[25] See https://ghostarchive.org/archive/TSSYx and https://ghostarchive.org/archive/9Q6GW.

[26] For example, "*lobs*" (@*unclelobs*), an account targeted among French media outlets, which was probably confused with @*Le_NouvelObs*. See https://perma.cc/AAX7-SVQU.

2.2 Patently inaccurate or misleading content

2.2.1 Misleading and untruthful content aimed at discrediting Ukraine and its allies

This campaign first seems to have appeared on September 5, 2023,[27] with a first post sharing a report impersonating *Fox News* and asking various media outlets to check the information.

The *Matryoshka* campaign then primarily involved dissemination of false graffiti and posts spoofing the visual identity of Western media outlets, institutions and NGOs using the above procedure. To date, this content has been published in French, English, Italian, German, Russian and Ukrainian.

Matryoshka spreads three types of content impersonating media outlets, institutions and NGOs:

- video reports with untruthful content using the visual identity and fonts of the organization. These false reports appear to be produced using royalty-free stock images and music;[28]
- False screenshots presenting an excerpt of an article, an *Instagram* story or a short *YouTube* video from a media outlet, organization or individual;
- Fake official documents impersonating a government body.

Other posts involve disseminating fake images of graffiti in the streets of major Western cities. These graffiti images are produced using a montage of a photograph of a real place and a caricature targeting Ukrainian or European figures. These manipulated images may also spoof the visual identity of street artists, like the French artist Lekto.

The narratives pushed by these publications primarily target Ukraine and aim to discredit its government and President, or else to criticize the arrival of Ukrainian refugees in Western countries. For example, many instances of fake graffiti, often anti-Semitic, depict Volodymyr ZELENSKYY as a beggar or war criminal, and several false reports have presented Ukrainian refugees in Europe in an unfavourable light[29] (see below).

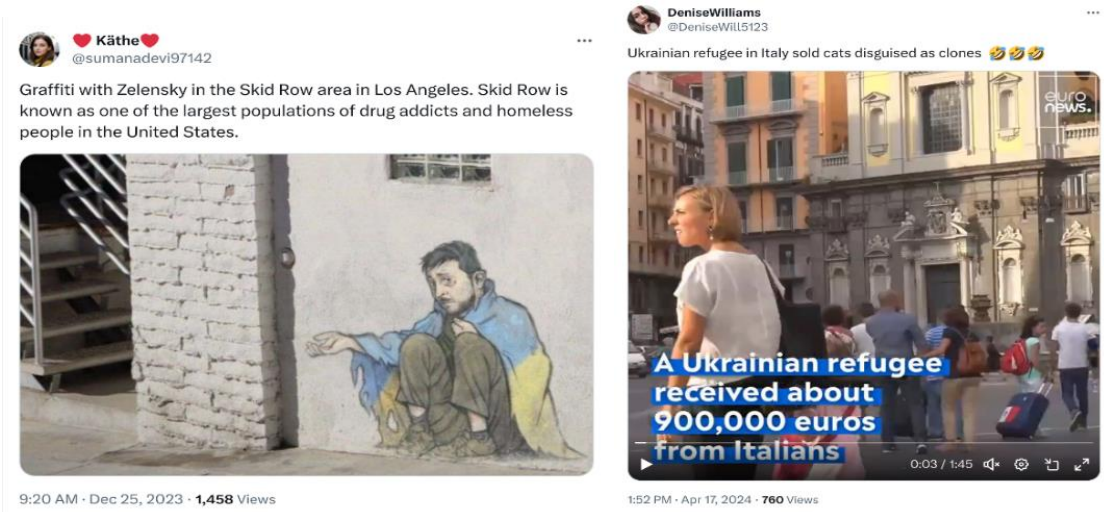

Fig. 4: Screenshots of fake graffiti depicting Volodymyr ZELENSKYY and a false report criticizing Ukrainian refugees

[27] https://archive.ph/4K6Oj.

[28] See article by the Russian outlet Provereno: https://provereno.media/blog/2024/05/11/krysy-klopy-tuberkulyoz-i-finansovye-problemy-feyki-rossyskoy-propagandy-ob-olimpiade-v-parizhe/.

[29] See archive of fake graffiti depicting Volodymyr ZELENSKYY (https://archive.ph/VEFVh) and a false report impersonating Euronews (https://archive.ph/XMWb6).

2.2.1 France, a key target of the *Matryoshka* campaign

Other narratives aim to discredit European governments, and particularly their policy supporting Ukraine. As such, France constitutes a key target for the campaign's operators.

Fig. 5: Screenshot of fake graffiti depicting Emmanuel Macron

The media outlets *BFMTV*, *Le Parisien*, *Libération*, *Le Monde* and *La Montagne*, as well as the Banque de France, the city of Paris and the Directorate-General for Internal Security (DGSI) have been impersonated by the *Matryoshka* campaign. Moreover, several cases of fake graffiti purported to be situated in and around Paris. This false content targeting France spread several narratives aimed notably at sowing distrust of French institutions and government members.[30]

Moreover, VIGINUM has observed that many *Matryoshka* operations have targeted the organization of the 2024 Olympic and Paralympic Games. These information operations impersonated media and institutions to spread the idea that the 2024 Games will be a failure among both French and international audiences. For instance, posts have spoofed the visual identity of the CIA[31] to claim that the terrorist threat was too high for the events to run smoothly, while a falsified Paris City Hall document in order to ask Parisians not to use their air conditioning as it would emit waves that could interfere with drones securing 2024 Games infrastructure (see below).

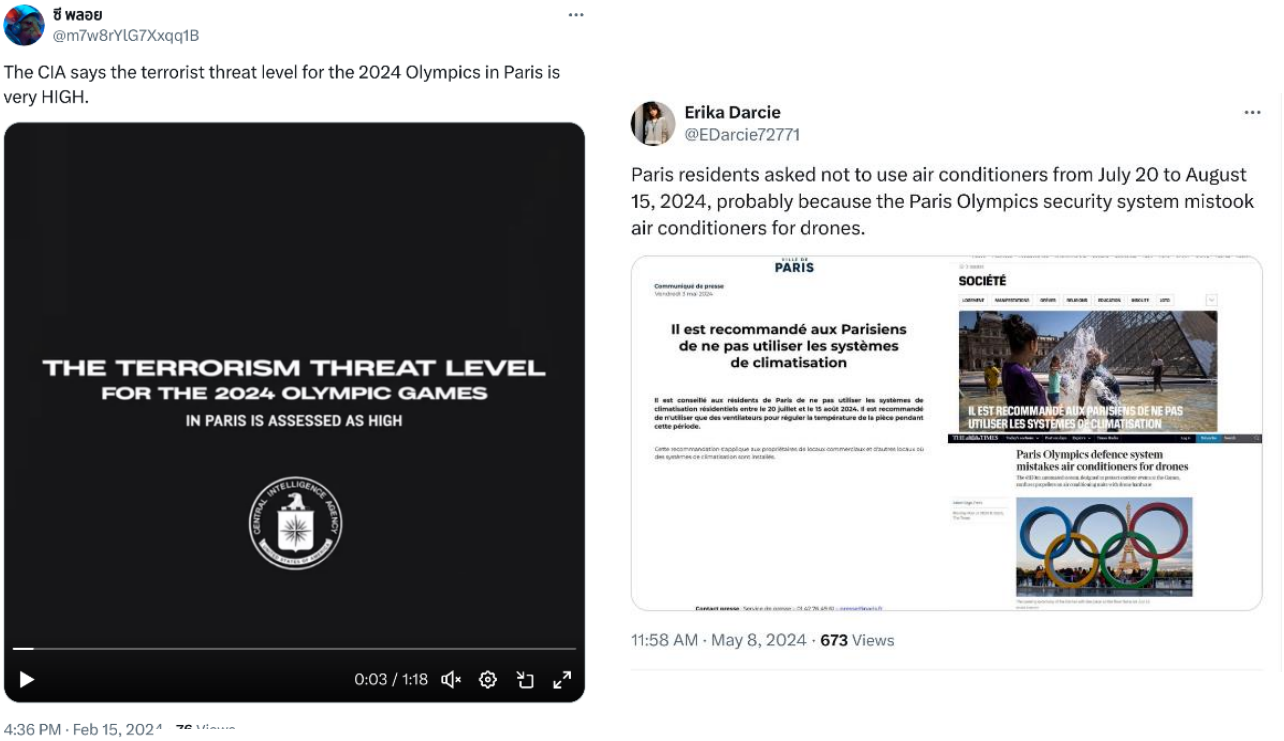

Fig. 6: Screenshot of posts targeting the 2024 Games

[30] For example, *Matryoshka* pushed narratives depicting the President of the Republic as being responsible for escalation of tensions with Russia (https://archive.ph/1Lx92) and accusing French law enforcement of sexual assaults during tensions in New Caledonia (https://archive.ph/ZqhAG).

[31] https://blogs.microsoft.com/on-the-issues/2024/06/02/russia-cyber-bots-disinformation-2024-paris-olympics/.

Lastly, on February 7 2024, the *Matryoshka* campaign stood out in disseminating a video presented as a montage by the French far-right student organization Groupe Union Défense (GUD) threatening to "burn down the Banque de France" because it was "lying" about its solvency (see below). This "false flag" video was part of a wider operation to discredit the Banque de France by impersonating both it and the DGSI to encourage people to withdraw massive amounts of cash.

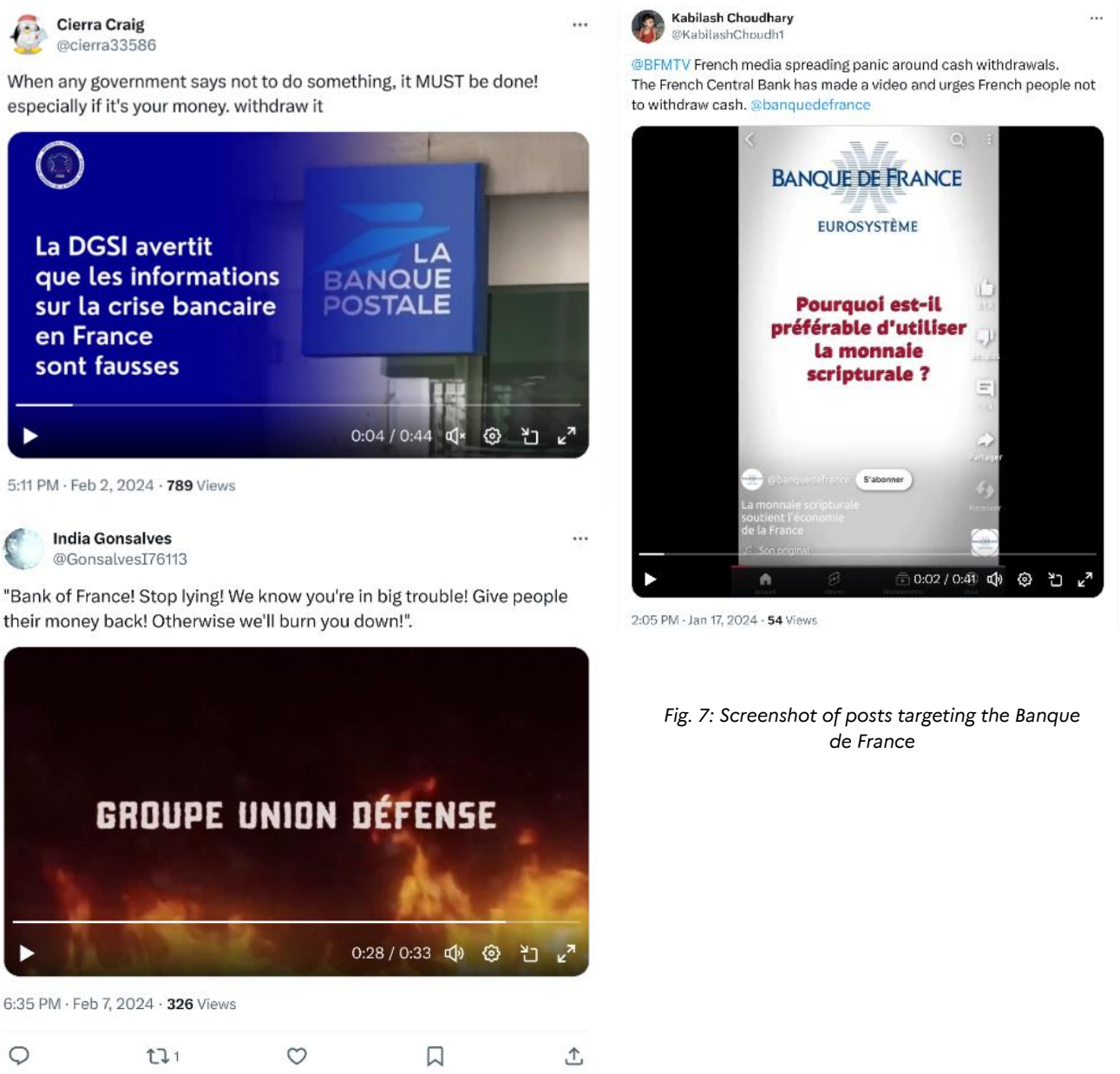

Fig. 7: Screenshot of posts targeting the Banque de France

In its analysis, VIGINUM has confirmed the dissemination of false or inaccurate allegations aimed at misleading web users.

2.3 Direct or indirect involvement of a foreign actor

VIGINUM investigations confirmed that the content released on *X* was issued upfront on Russian-speaking *Telegram* channels (see annex 3.3). With one exception, fake reports, screenshots and graffiti seem to have been first posted by channels like *@sheyhtamir1974*, *@belshkarvka* and *@thehandofkremlin*, and uploaded within a relatively short time span.[32] All this suggests that the content was initially set up for Russian-speaking audiences.

While the administrators of the three abovementioned channels appear different and have their own editorial lines, original publications in Russian, associated with misleading content, have often been copypastas,[33] which are identifiable through specific headers.

Semantic analysis of messages published between February 22, 2022 and May 10, 2024 by the channels *@sheyhtamir1974*, *@belshkarvka* and *@thehandofkremlin*, with at least one of these two headers, in Russian: "#нам_пишут_наши_любимые_подписчики" ("#our favourite subscribers have written to us") and "#от_подписчика" (" #from a subscriber"), demonstrated the frequency with which the copypasta technique is used by these three channels, and the increase in the amount of fake content since September 2023.

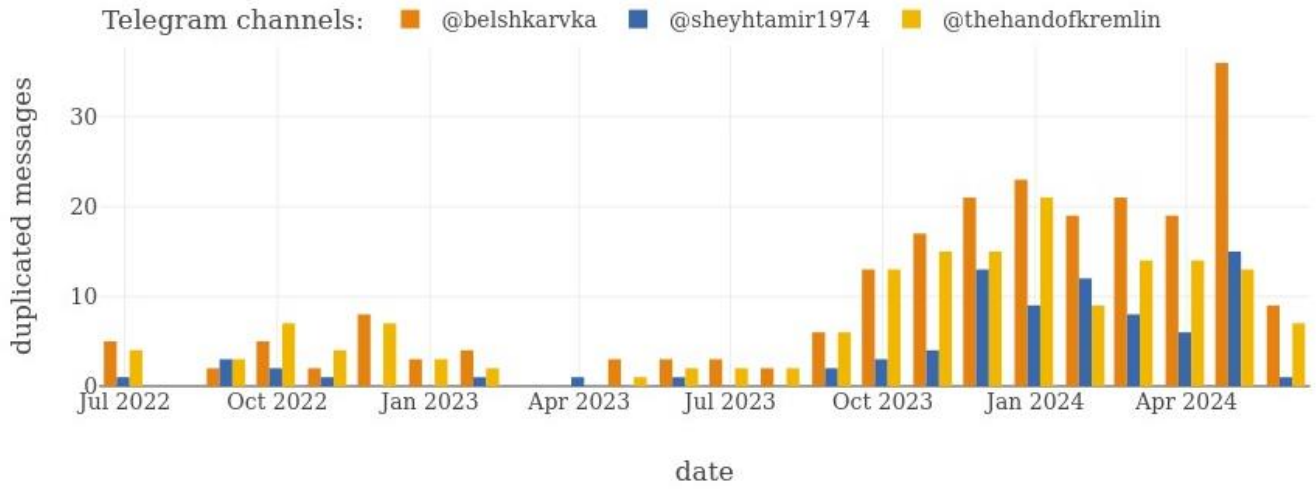

Fig. 8: Graph of copypastas of misleading messages published on Telegram channels

In light of this, VIGINUM suspects that this content was created by third parties in order to be posted on *Telegram* through coordinated action. For now, there is no technical evidence linking *Matryoshka*'s operating methods to third parties who may have designed content posted by the channels.

The theory that third parties were involved seems to be supported by the fact that the administrators of these channels are likely to have been remunerated for publishing "political content", which is a common practice in the ecosystem of pro-Kremlin channels, according to an investigation by Russia media outlet *Proekt*[34]. For example, the *@thehandofkremlin* channel invites users to contact an intermediary known as "Sergey KALASHNIKOV" for all commercial partnerships. Furthermore, Sergey KALASHNIKOV runs a Russian-language *Telegram*[35] channel, where he proposes to publish content against payment on *Telegram* channels that had already been identified in previous information operations (see below).

Finally, the *RRN* campaign has already published false reports which are very similar those published by *Matryoshka* in the previous operations[36], leading to the assumption that this content was created by the

[32] https://archive.ph/PHjTq.
[33] A block of text or a visual which is identically or almost identically copied and pasted, on one or several web platforms, with the aim of making a message more visible.
[34] https://www.proekt.media/narrative/telegram-kanaly/.
[35] https://t.me/together_to_the_stars.
[36] On March 18 and 19, 2023, sponsored content from the RRN campaign released a video on *Facebook* which impersonated the *Le Figaro* newspaper, claiming that Nord Stream had been sabotaged by the United States and the United Kingdom (ad ID:

same actors. This idea is backed by the fact that, according to documents published by the *Washington Post*,[37] the *Telegram* channel @*sheyhtamir1974* appears several times on the dashboard of a user known as "Center S".[38] According to that article, the Center could have links with the Russian Presidential Administration and could be responsible for coordinating "influence operations" against foreign countries. Furthermore, again from the *Washington Post*, the Russian Presidential Administration is suspected to have sub-contracted part of its work to *ASP* and *Struktura*, both of which have been publicly accused of being behind the *RRN* campaign[39].

Thus, the systematic use of Russian channels as channels of first release, as well as the publication of original Russian-language content, form a body of corroborating evidence to suggest the involvement of a foreign actor.

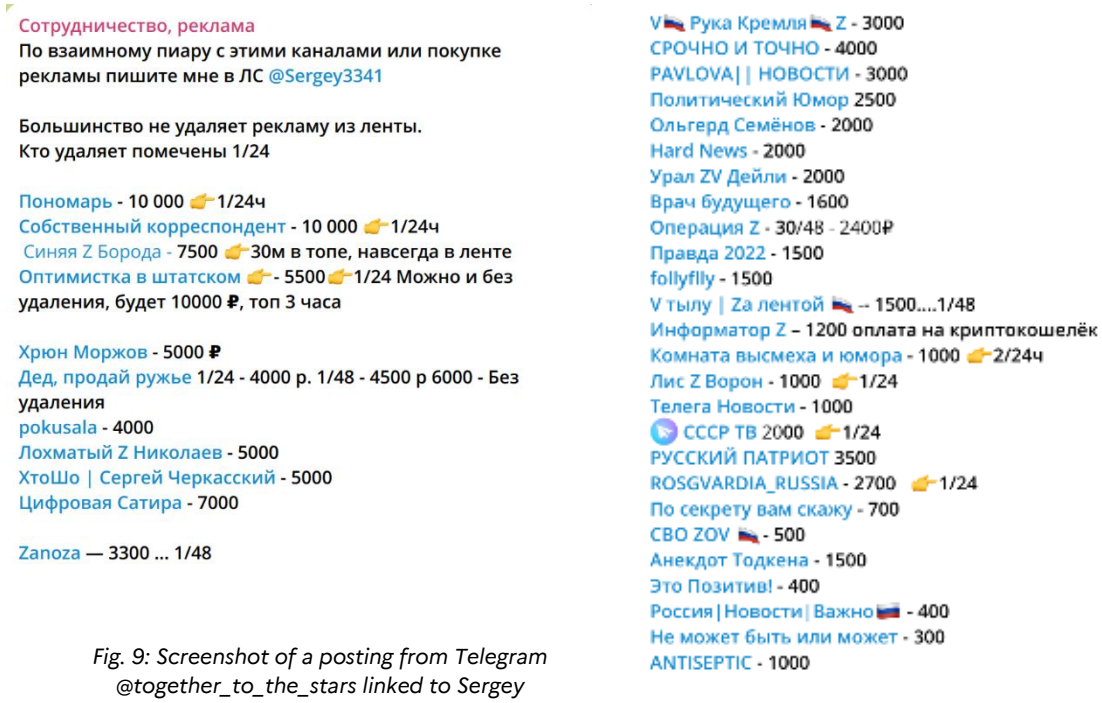

Fig. 9: Screenshot of a posting from Telegram @together_to_the_stars linked to Sergey Kalashnikov and offering paid partnerships with Telegram channels

4208250569399286). On 21 October 2023, a network of now-suspended *X* accounts from the RRN campaign published a report which also impersonated *Le Figaro*, claiming that Israel was using fake videos to justify its action in the Gaza Strip (https://twitter.com/casusbellii/status/1716429778956189928).

[37] https://www.washingtonpost.com/world/2024/02/16/russian-disinformation-zelensky-zaluzhny.

[38] https://archive.ph/y1UvB, https://archive.ph/YFeUX and https://archive.ph/B5gDP.

[39] See: https://about.fb.com/news/2022/11/metas-adversarial-threat-report-q3-2022/.

2.4 Attack on France's fundamental interests

VIGINUM believes that the main goal of the *Matryoshka* campaign is to discredit Western personalities and media outlets involved in fact-checking, including publicly, if they react to fake content. At this point, seeking an audience seems to be only a secondary goal for operators, as can be seen with the low audience volumes and weak engagement in campaign publications,[40] and despite the operating method being used against hundreds of entities.

Analysis of those who first release content suggests that content initially aimed for a Russian audience is picked up by *Matryoshka*, and then re-used at minimal cost against "Western" targets. In certain cases, media outlets have effectively responded to calls from quoters, or even analysed and published articles on content released during the campaign, thus exposing themselves to large-scale targeting aimed at saturating their investigative abilities.

VIGINUM believes that this campaign undermines the reputation of French mainstream media and official institutions. Since the start of the large-scale invasion of Ukraine in February 2022, the Russian influencing mechanism has regularly targeted fact-checkers[41] and used extensive resources to discredit analysis from Western media outlets.

Furthermore, the use of the President of the French Republic's image for disinformation purposes as well as repeated attacks against the 2024 Olympic and Paralympic Games and the French policy in support of Ukraine are most likely aimed at damaging France's international reputation among particular audiences. After this analysis, VIGINUM believes that the *Matryoshka* campaign is likely to directly undermine France's fundamental interests.

* * *

Given the coordinated and unauthentic release methods, the misleading and deceptive nature of the *Matryoshka* postings, probable links between the campaign and Russian actors and the clear intention to damage France's image, **the criteria of a foreign digital interference appear to have been met**.

Furthermore, VIGINUM believes that its operating methods could change in the months ahead to make its procedures stealthier, trap more targets and reach a wider audience.

[40] For example, the operation aiming to send a fake piece of Lekto graffiti to 162 *X* accounts launched on 24 April 2024 had only received 720 views as of 2 May 2024.

[41] See specifically: https://dfrlab.org/2022/05/04/how-russia-employs-fake-fact-checking-in-its-disinformation-arsenal.

3. APPENDIX

3.1 Tactics, techniques & procedures

[TA01] Plan Strategy
- [T0074] Determine Strategic Ends

[TA02] Plan Objectives
- [T0002] Facilitate State Propaganda
- [T0066] Degrade Adversary
- [T0075] Dismiss
- [T0075.001] Discredit Credible Sources
- [T0076] Distort
- [T0077] Distract
- [T0079] Divide

[TA13] Target Audience Analysis
- [T0072] Segment Audiences
- [T0072.001] Geographic Segmentation
- [T0081] Identify Social and Technical Vulnerabilities
- [T0081.003] Identify Existing Prejudices
- [T0081.004] Identify Existing Fissures
- [T0081.005] Identify Existing Conspiracy Narratives/Suspicions
- [T0081.008] Identify Media System Vulnerabilities

[TA14] Develop Narratives
- [T0003] Leverage Existing Narratives
- [T0004] Develop Competing Narratives
- [T0022] Leverage Conspiracy Theory Narratives
- [T0022.001] Amplify Existing Conspiracy Theory Narratives
- [T0022.002] Develop Original Conspiracy Theory Narratives
- [T0040] Demand Insurmountable Proof
- [T0068] Respond to Breaking News Event or Active Crisis
- [T0083] Integrate Target Audience Vulnerabilities into Narrative

[TA06] Develop Content
- [T0019] Generate Information Pollution
- [T0023] Distort Facts
- [T0023.001] Reframe Context
- [T0023.002] Edit Open-Source Content
- [T0084] Reuse Existing Content
- [T0084.002] Plagiarise Content
- [T0084.003] Deceptively Labelled or Translated
- [T0086] Develop Image-Based Content
- [T0086.003] Deceptively Edit Images (Cheap Fakes)
- [T0087] Develop Video-Based Content
- [T0087.002] Deceptively Edit Video (Cheap Fakes)

[TA15] Establish Social Assets
- [T0090] Create Inauthentic Accounts
- [T0090.001] Create Anonymous Accounts

[TA16] Establish Legitimacy
- [T0099] Impersonate Existing Entity
- [T0099.002] Spoof/Parody Account/Site
- [T0099.003] Impersonate Existing Organisation
- [T0099.004] Impersonate Existing Media Outlet
- [T0099.005] Impersonate Existing Official
- [T0099.006] Impersonate Existing Influencer

[TA07] Select Channels and Affordances
- [T0104] Social Networks
- [T0104.001] Mainstream Social Networks
- [T0112] Email

[TA09] Deliver Content
- [T0115] Post Content
- [T0116] Comment or Reply on Content

[TA11] Persist in the Information Environment
- [T0128] Conceal Information Assets
- [T0128.001] Use Pseudonyms
- [T0128.004] Launder Information Assets
- [T0129] Conceal Operational Activity

[T0129.002] Generate Content Unrelated to Narrative

3.2 Impersonated French entities & media outlets

Target	Online archive[42]	Date
Le Parisien	https://archive.ph/8kQmd	21 September 2023
La Montagne	https://archive.ph/oCZmb	9 October 2023
Le Monde	https://archive.ph/pefZ7	16 November 2023
RFI	https://archive.ph/9I6ZG	24 November 2023
DGSI	https://archive.ph/vFEsk	2 February 2024
Le Figaro	https://archive.ph/0d6l3	8 March 2024
France 24	https://archive.ph/PdIVl	28 March 2024
France 24	https://archive.ph/1SW5K	11 April 2024
Le Figaro	https://archive.ph/MndmD	12 April 2024
RFI	https://archive.ph/rta16	15 April 2024
RFI	https://archive.ph/sVNOk	18 April 2024
RFI	https://archive.ph/WvAl3	19 April 2024
BFMTV	https://archive.ph/kTtES	8 May 2024
BFMTV	https://archive.ph/Wb5VG	8 May 2024
City of Paris	https://archive.ph/N2OzX	8 May 2024
Libération	https://archive.ph/biAIN	11 May 2024
BFMTV	https://archive.ph/NGyE8	13 May 2024

3.3 Examples of campaign content released

Content	Telegram channel on which it was first released	Release date	*Matryoshka* "seeder" accounts on *X*	Release date
Report by *Der Spiegel* on a goalkeeper	https://archive.is/a0R2H	Sunday, 28 April 2024 at 19:01	https://archive.is/dkk0k	30 April 2024 at 12:30
Report by *BFMTV* on Eurovision	https://archive.is/w6ejq	Saturday, 11 May 2024 at 10:07	https://archive.is/1GmF8	13 May 2024 at 12:39
Anti-Semitic graffiti in Paris	https://archive.is/P2nMD	10 May 2024 at 15:37	https://archive.is/hAH62	15 May 2024 at 13:34

[42] These archives were communicated to us by antibot4navalny.

ABOUT VIGINUM

Created on 13 July 2021 and attached to the General Secretariat for Defence and National Security (SGDSN), France's service for vigilance and protection against foreign digital interference (VIGINUM) is intended to protect the online public debate which affects France's fundamental interests.

This technical and operational state agency is responsible for monitoring and defining information manipulation campaigns on digital platforms, involving foreign actors with the aim of damaging France and its interests.

Service for vigilance and protection against foreign digital interference | SGDSN

Cover photo credit: flickr | www.CGPGrey.com; photo cropped and converted to black and white