PREMIÈRE MINISTRE

*Liberté*
*Égalité*
*Fraternité*

Secrétariat général de la défense et de la sécurité nationale

VIGINUM

# ***RNN*:**
# A complex and persistent information manipulation campaign

Summary

13 June 2023

Since spring 2022, VIGINUM has identified a digital information manipulation campaign targeting several European States, including France. This campaign aims to undermine Western support for Ukraine, mainly by spreading the narrative that Western populations would allegedly support Russia. Because of the central role of the media *Reliable Recent News*, the main source of the above-mentioned narrative, this campaign has been named *RRN*.

Particularly persistent, the *RRN* campaign relies on several modus operandi:

- Creating websites which share audio-visual content criticizing Ukrainian leaders:
- Impersonating the identity of national media outlets and European governmental websites via typosquatting their domain name[1];
- Creating French-speaking news websites which share controversial content leveraging French national news;
- Creating networks of inauthentic accounts, mainly on *Facebook* and *Twitter*, in order to spread the content published on the domain names registered in the context of the campaign.

On 15 December 2022, following the publication of several reports a few months earlier, by the NGO *EU DisinfoLab*[2], the *Institute for Strategic Dialogue* (ISD)[3] and the Atlantic Council's *Digital Forensic Research Lab* (DFRLab)[4] , *Meta* publicly attributed the *RRN* campaign to two Russian companies: *ASP* and *Struktura*.

Investigations conducted by VIGINUM have uncovered several elements pointing to the involvement of Russian or Russian-speaking individuals and several Russian companies in the design and conduct of this campaign. VIGINUM has also observed that several government entities or entities affiliated with the Russian Federation participated in spreading some contents.

[1] Typosquatting is a modus operandi when people register domain names with deliberately misspelled names of well-known websites to deceive unsuspecting users. In this case, a website has been cloned except for a few details, generally unnoticeable to the general public, so that users think it is an official website.

[2] Doppelganger - Media clones serving Russian propaganda - EU DisinfoLab, 27 September 2022.

[3] Pro-Kremlin Network Impersonates Legitimate Websites and Floods Social Media with Lies, ISD, 29 September 2022.

[4] Russia-based Facebook operation targeted Europe with anti-Ukraine messaging, DFRLab, 27 September 2022.

## Dissemination of pro-Russian and anti-Western content related to the war in Ukraine

The information manipulation campaign detected by VIGINUM mainly targets Ukraine and its allies, who are criticized through multiple manifestly inaccurate or misleading allegations. The *RRN* campaign is focused on four main themes: (1) The alleged ineffectiveness of sanctions targeting Russia, which would above all negatively impact European States and/or their citizens; (2) The alleged Russiaphobia of Western States; (3) Barbaric acts allegedly committed by Ukrainian armed forces, and the neo-Nazi ideology that would predominate among Ukrainian leaders; (4) The negative effects on European States that would allegedly be generated by the hosting of Ukrainian refugees.

For instance, manifestly inaccurate or misleading narratives disseminated under the *RRN* campaign alledged that France was implicated in war crimes because of its supply of CAESAR truck-mounted howitzers to Ukraine. Other published content claimed that a radioactive cloud was headed towards France because the United Kingdom gave Ukraine shells containing depleted uranium.

Moreover, the *RRN* campaign attempts to erode the support of the people in Western States for Ukraine. In addition to criticizing European political positions, the campaign also aims to convince the Russian audience of the alleged support of Western populations to Russia. VIGINUM has therefore observed that some content produced was shared by Russian government media outlets.

The *RRN* campaign also uses constantly satirical cartoons about the conflict in Ukraine that are very critical of Western States. The main source of these satirical cartoons is the *Telegram* channel, *@VoxCartoons*, created on 2 April 2022. The campaign also relies on satirical cartoons found on the website *memhouse[.]online*, created on 15 April 2022 and hosted in Russia.

## A campaign relying on several modus operandi

### Creation of fake media outlets disseminating pro-Russian and anti-Western content

The campaign is conducted via the media *RRN*, created on 10 March 2022, a few days after Russia's "special military operation" was deployed in Ukraine. This media outlet develops an editorial line focusing on the four themes mentioned above.

The investigations conducted by VIGINUM uncovered technical links between *RRN* and the fake fact-checking platform, *War on Fakes*[5], that was launched a few hours after the invasion of Ukraine, on 24 February 2022, and became widely known through coordinated efforts of the Russian diplomatic network[6]. The *RRN* campaign also relies on three websites, *truemaps[.]info, tribunalukraine[.]info* and *ukraine-inc[.]info*, which aim to accuse Ukraine and its allies of having committed war crimes and of benefitting financially from the conflict.

At the same time, on 6 April 2022, the multi-lingual website, *newsroad[.]online, similar to RRN in terms of content and appearance,* was registered online.

VIGINUM has also detected since summer 2022 the creation of several fake European news websites affiliated with the *RRN* campaign. As such, the *avisindependent[.]eu* website, which claims to be a media publishing "news and analyses on the war in Ukraine", was created, along with four other fake media outlets affiliated with *newsroad[.]online*[7].

On 24 February 2023, one year to the day after Russia invaded Ukraine, five additional websites were created[8]. Using names that sound French, like *La Virgule*, *Allons-y* or *Notre Pays*, these websites

[5] *War on Fakes* is a fake fact-checking multilingual platform used by Russia to deny the accusations that Russia has committed war crimes since it invaded Ukraine. The domain name *waronfakes[.]com* was registered by Timofey Vasiliev, a former employee of a company affiliated with the Russian Presidential Administration.

[6] Including the official page of the Russian Ministry of Foreign Affairs on *Facebook*, and the Russian Embassy in France.

[7] *Viedo-klis[.]lv*, *librelepresse[.]fr*, *weltereignisse365[.]de*, *libera-stampa[.]*it.

[8] *allons-y[.]social*, *candidat[.]news*, *notrepays[.]today*, *franceeteu[.]today*, *lavirgule[.]news*.

presenting themselves as French-language news media outlets publish polarizing articles about French and European political life.

### Impersonating the identity of foreign media outlets and government websites

VIGINUM observed the registration between June 2022 and May 2023 of 355 domain names impersonating the identity of media outlets in France and in nine states of Europe, the Americas and the Middle East. This typosquatting technique was used to disseminate pro-Russian articles related to the war in Ukraine by having them appear to be articles published by legitimate media outlets.

In France, four media outlets were affected by these tactics: *20 Minutes*, *Le Monde*, *Le Parisien* and *Le Figaro*[9]. The investigations conducted by Viginum highlighted the existence of at least 49 false articles in *Le Parisien*, seven in *20 Minutes*, one in *Le Figaro* and one in *Le Monde*.

From the end of May 2023, malicious actors working on the *RRN* campaign pushed forward their modus operandi by impersonating, *via* the typosquatting of domain names, the identity of the website of the French Ministry for Europe and Foreign Affairs (MEAE). The sub-domain *diplomatie.gouv[.]fm* was thus used to publish a false official document stating that France had introduced a "security tax" for the benefit of Ukraine. The same method was used to impersonate the identity of the Interior Ministry of Interior of a foreign country in order to suggest the creation of a mandatory programme for citizens to welcome Ukrainian refugees.

### Use of inauthentic accounts on social media

During summer 2022, more than 30 social media accounts were created to increase the visibility of the *avisindependent[.]eu* and *RRN* websites. These accounts shared *URLs* towards the two websites, along with pro-Russian, anti-Western and anti-Ukrainian caricatures.

At the same time, Viginum observed that a group of almost 200 single-use Facebook accounts had been created, set up to publish one single post, targeting French and European audiences. These accounts, most of which were named "Open Opinion" used the logo of foreign media outlets or AI-generated images as profile pictures. Through sponsored content, they shared *URLs* redirecting to articles published on *RRN* and to typosquatted domain names of foreign media outlets.

From early 2023, the modus operandi of the *RRN* campaign changed on Facebook in order to bypass the moderation rules set up by *Meta*. Thus, Viginum detected a network of over 160 Facebook pages, disseminating over 600 items of sponsored content including URLs redirecting to articles and websites included in the scheme. These URLs were set up to redirect traffic several times before reaching their target site, so as not to reveal the entire infrastructure put in place under the campaign.

Finally, since the end of May 2023, Viginum has observed a network of *Twitter* bots[10] which use the reply field in tweets published by European media outlets and political figures to post URLs redirecting to sites included in the *RRN* campaign. As on Facebook, the shared URLs are programmed to redirect several times.

## Numerous signs of involvement from Russian actors

### *Meta* attributes the campaign to two Russian companies

On 15 December 2022, *Meta* publicly attributed the *RRN* campaign to two Russian companies: *Structura National Technologies* (*Struktura*) and *Social Design Agency* (*Agentstvo Sotsialnogo Proektirovania*). These two digital marketing companies, which provide services to several Russian government institutions, are run by Ilya Andreevich Gambachidze. This well-known political strategist from Moscow was notably deputy prefect for the Northern Moscow administrative district and adviser to the Deputy Chairman of the State Duma, Petr Tolstoy.

[9] *20minuts[.]com, lemonde[.]ltd, leparisien[.]ltd, lefigaro[.]me.*

[10] According to Cloudflare, a bot is a software application programmed to carry out certain automated tasks online, without the need for a human user to manually activate them each time.

### Involvement of several Russian nationals

The open-source investigations conducted by Viginum uncovered the involvement of several Russian individuals and companies in carrying out the *RRN* campaign. They found that the *avisindependent[.]eu* domain name was registered under Mikhail Andreevich Tchekomasov. Co-founder of *Hustle Media* (Хасл Медиа), specializing in the management of influencers on social media and blogs, Mikhail Andreevich Tchekomasov is also co-founder of *IPTeam*, a company already identified as having tried to approach French influencers so that they spread favourable content for Russia in the context of the war in Ukraine[11]. At the same time, Russian citizen Andrey Chubotchkin was identified as having registered several domains included in the *RRN* network[12].

### Active involvement of the Russian diplomatic network

The Russian diplomatic network has on several occasions participated in sharing and, de facto, amplifying the *RRN* campaign since the spring 2022. Seven official Facebook accounts of Russian embassies in the Indian sub-continent shared URLs directing directly to the rrn[.]world site. Furthermore, nine official "Russian Houses"[13] Facebook pages were involved in distributing cartoons published by *ukraine-inc[.]info*.

Finally, some of the caricatures broadcasted on the *Telegram* @*VoxCartoons* channel and spread as part of the *RRN* campaign had been shared by the *Twitter* account of the Russian Embassy in France on 23 March 2022, i.e. more than a week prior to the creation of the *Telegram* channel.

## Assessment of the attack on the fundamental interests of the nation

The *RRN* campaign is a widespread foreign digital interference, notably involving, in a coordinated way, groups of inauthentic accounts on social media and websites impersonating the identity of government institutions and French and foreign media outlets. Its main goal appears to be to use inauthentic and unfair means to criticize the policy of the West, particularly that of France, with regard to the Ukrainian conflict (delivery of weapons to Ukraine, consequences of Western sanctions against Russia, welcoming Ukrainian refugees) as well as its coverage by major national media outlets.

The *RRN* campaign stands out for its persistent nature. Despite being publicly exposed on various occasions by civil society actors and despite the different moderation measures taken by the *Meta* group and by *Twitter*, it remains active. By regularly changing its methods, it seeks to bypass any measures taken against it.

In view of the modus operandi implemented and the objectives pursued by this campaign, Viginum considers that the detected phenomenon threatens the fundamental interests of the nation.

[11] https://www.marianne.net/monde/europe/guerre-en-ukraine-une-operation-dinfluence-russe-vise-des-youtubeurs-francais
[12] *memhouse[.]online*, *newsroad[.]online*, *urlbox[.]online*.
[13] "Russian Houses" are institutions attached to the Federal Agency for the Commonwealth of Independent States Affairs, Compatriots Living Abroad, and International Humanitarian Cooperation (Rossotrudnichestvo), which is Russia's main soft power and public diplomacy institution.