GOUVERNEMENT

Liberté
Égalité
Fraternité

RUSSIAN DISINFORMATION: THE BETTER WE KNOW IT, THE BETTER WE CAN RESPOND

Press kit

Introduction

Today, in international conflicts, disinformation has undeniably become a weapon of war, using lies hidden in our daily news stream in an attempt to distort facts.

Disinformation is used to sow doubt and create tensions in our societies. This is what Russia, using the RRN/ Doppelgänger network, did in November 2023 when spreading and artificially amplifying graffiti of Stars of David tagged on walls in Paris. The people behind these campaigns stir up hatred and seek to pit us against one another, here in our own country.

Russia is not the only disinformation actor, but it uses financial resources and methods that make it stand out. Since 24 February 2022, Russia's information attacks have not only intensified, but they have also changed in nature. The war of aggression against Ukraine is expanding into an information war against Ukraine and all the countries that support Ukrainians.

To address the threat from Russian disinformation to the European elections in June 2024, European governments must anticipate, monitor, characterize and condemn manoeuvres and information manipulation.

France has organized its response to disinformation nationally and internationally, with a partnership-based approach.

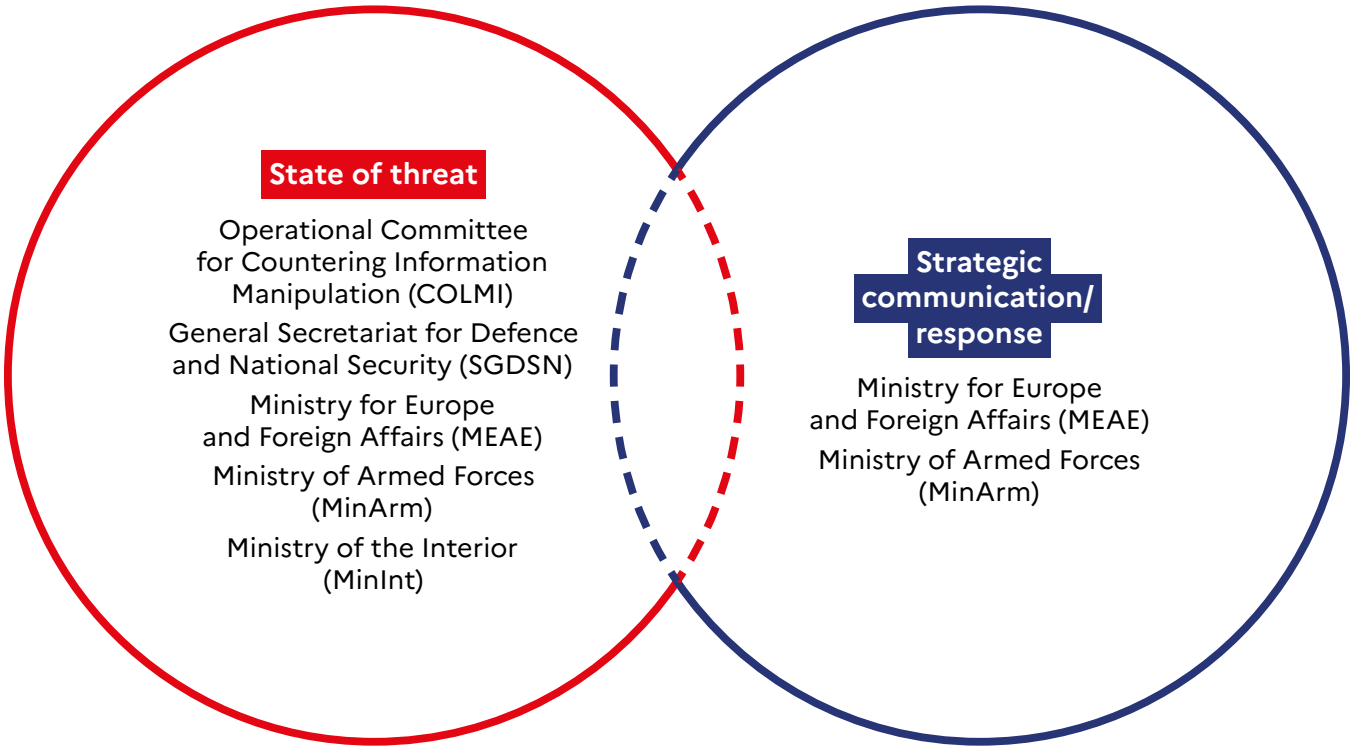
France is ready

The French response to foreign digital interference, and particularly that of Russia, involves all government actors, which closely coordinate their efforts.

A particular feature of the French system is that it has both a specialized agency for online investigation (VIGINUM) and a task force dedicated to the response to information crises (MEAE/EMA), so it can cover a very broad spectrum.

The strength of our response also lies in staying true to our values and our democratic principles.

International cooperation



France has been building strong momentum with its European partners

We are bolstering our efforts to fight foreign digital interference and manipulation of information, particularly within the European Union.

Within the European Union, the Foreign Affairs Council deals with fighting foreign interference and manipulation of information (FIMI) at a political level. The decisions made there are translated into tangible action conducted by the European external action service (EEAS) StratCom team, which has been developing a toolbox over the past two years to tackle hybrid threats.

The EEAS, a pioneer in setting analytical standards about FIMI, has introduced a rapid alert system so that Member States can report incidents and share investigations on foreign digital interference. The EEAS has also developed a EUvsDisinfo website that explains Russian manoeuvres.

These responses are to be accompanied by progress in moderating content on social media. Digital platforms have a responsibility in selecting content through their algorithms. France and its European partners are working with the private sector to fight disinformation.

The implementation of the EU's Digital Service Act since 25 August 2023 is a major step forward in helping the companies concerned to strengthen their standards in the area. But we need to do more to drive these companies to moderate and to do so in more languages.

Digital Services Act: : this regulation on digital services regulates intermediaries and online platforms such as marketplaces, social networks, content-sharing platforms, app stores and online travel as well as accommodation platforms. Its main objective is to prevent illegal and harmful activities online and the spread of disinformation. It ensures user security, protects fundamental rights and creates a fair and open platform environment.

(Source: European Commission/ https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en *)*

Understanding Russian disinformation to better address it

Digital interference from Russia is not new. Incidents have been increasing in Europe and the United States since 2014 and the illegal annexation of Crimea.

This hybrid strategy reached unprecedented levels after 24 February 2022 and the start of Russia's war of aggression against Ukraine. In June 2023, French authorities exposed a digital information manipulation campaign against France, involving Russian actors (see below). Since then, France has condemned several Russian digital interference operations and the European Union has imposed sanctions on several Russian individuals and entities linked to information manipulation campaigns.

Information manipulation and disinformation manoeuvres by Russian actors currently serve well identified strategic objectives: to legitimize Russia's war of aggression against Ukraine, to undermine the cohesion of support for Ukraine, and to destabilize the societies of liberal democracies.

These actions target Ukraine first and foremost, but also Western public opinion and leaders as well as public opinions in third countries, particularly in sub-Saharan Africa. Russia has also recently stepped up its disinformation action in other regions, such as Latin America.

Traditional Russian *modus operandi*

Creation of media outlets, foundations and think tanks controlled by Russian actors. For example, the Foundation to Battle Injustice is directly managed by the influential structures of Yevgeny Prigozhin's Project Lakhta.

Use of hundreds of thousands of inauthentic social media accounts belonging to fake users who post and share anti-West and pro-Russia content. Some accounts are managed by troll farms, and others run automatically as bot accounts.

Hidden placement of publications: this is a practice used by both state and private Russian disinformation actors. It involves having legitimate media outlets publish "ready to use" articles that are favourable to Russian interests in exchange for payment. This modus operandi, like corruption, enables Russia to circumvent:

→ The rules adopted by fact-checking bodies;

→ The detection mechanisms of social media platforms that aim to fight information manipulation;

→ French and European Union sanctions on recognized Russian propaganda entities such as Russia Today or Sputnik.

For example, Project Lakhta gets several thousands of articles published a year, in different languages, in around 60 media outlets, including Western ones. In addition to the influence it seeks to have on local communities (for example support for a pro-Russia politician, criticism of Western action), these publications artificially create the impression that public opinion in various countries is in favour of Russia.

The mercenaries of Russian influence also rely on local intermediaries. These individuals, who often receive payment, may themselves believe ideologically and realize what they are doing. However, in other cases, these mercenaries achieve their ends by deceiving their interlocutors who are unaware that they are victims of the Russian propaganda machine.

More precisely, various Russian *modus operandi* for information manipulation have been identified since the Russian war of aggression on Ukraine began.

For several months, although the quality of the narratives has declined, **coordination of the various channels used for Russian information manipulation has improved.** Russian manoeuvres rely on a wide range of channels: imitation of official sources (fake Facebook pages of major international media outlets publishing real articles), Telegram channels and conspiracy networks, but also official channels and actions in the physical world (for example, Dmitry Rogozin sent to the French ambassador in Moscow, Pierre Lévy, a fragment of a shell fired from a Caesar howitzer that he claimed had been lodged in his spine).

Multilayer actions are now widespread: the first articles expressed false allegations on the basis of questionable evidence, a second wave of articles commented on the first articles, and so on, to the point that this fabricated information has now been included in official Russian stances at the highest level of the Russian Government. The objective is to flood the news space to create confusion.

"Fake fact-checking" has existed since 2014 and is now even more prevalent. It consists in debunking false allegations created for the occasion.

Unable to propose a credible counter-narrative (example of Bucha massacre), Russia has invented multiple alternative narratives to divert attention.

The timing of information operations is essential for determining the outcome. Narratives are spread at key moments of political debates in the targeted countries. These operations are often conducted during elections.

Since February 2022, Russian manoeuvres have multiplied in France's news space.

These manoeuvers are not all of the same nature, but they are all part of a clear strategy to identify and exploit the weak points in public debate. Three recent examples illustrate the different modes of action.

RRN (RECENT RELIABLE NEWS)

This information manipulation campaign aims to discredit Western support for Ukraine. Known as RRN due to the central role of the so-called Reliable Recent News media outlet, this campaign has four components:

— Dissemination of pro-Russian content related to the war in Ukraine, particularly criticizing the country's leaders;

— Spoofing websites of news outlets, and government and EU websites, using "typosquatting" to imitate their domain name;

— Creation of French-language news websites sharing controversial content in order to use French national news for their own ends;

— Use of combined inauthentic resources, such as fake websites or social media accounts , to spread content.

To do so, the RRN campaign uses a series of inauthentic narratives with four main themes. They aim to sow division and artificially arouse mistrust between civil society and its leaders:

— The alleged ineffectiveness of sanctions targeting Russia, which are allegedly negatively impacting European States and citizens the most;

— The alleged Russiaphobia of Western countries;

— The alleged barbaric acts committed by the Ukrainian armed forces, and the neo-Nazi ideology that is supposedly rampant among Ukrainian leaders;

— The negative effects that Ukrainian refugees are allegedly having on European States.

Some 355 domain names imitating media outlets were detected by VIGINUM, four of them targeting French speakers more specifically and copying the graphic identity of the French daily newspapers *20 Minutes, Le Monde, Le Parisien* and *Le Figaro*. At least 58 articles have been published via these channels.

In the course of its open source investigation, VIGINUM detected the involvement of Russian or Russian-speaking individuals and several Russian companies.

In late May 2023, the RRN campaign went further than ever before in spoofing the website of the French Ministry for Europe and Foreign Affairs.

STARS OF DAVID

France has condemned the involvement of the same Recent Reliable News (RRN/Doppelgänger) network in artificially amplifying photos of Stars of David in the 10th arrondissement of Paris and being the first to post them on social media a few days after the massacres perpetrated by Hamas on 7 October.

With regard to the acts themselves, the judicial investigation under way should establish the possible responsibility of a foreign entity who commissioned them.

With regard to their amplification, on 6 November 2023, VIGINUM, France's technical and operational agency responsible for monitoring and protecting against foreign interference online, detected the involvement of a network of 1,095 bots on X (formerly Twitter). These bots made 2,589 posts amplifying the Stars of David controversy. VIGINUM considers, with a high degree of confidence, that these bots are affiliated with the RRN scheme in that one of their main activities is redirecting readers to the websites of this scheme.

While the photos of the graffiti were first authentically posted on X on 30 October at 7:37 PM, VIGINUM found that the photos were first posted on the RRN bot network at 7:24 PM on 28 October, 48 hours before.

This latest Russian digital interference operation against France reflects the continuation of an irresponsible and opportunistic strategy aiming to exploit international crises to create confusion and tensions in public debate in France and Europe.

PORTAL KOMBAT

Between September and December 2023, VIGINUM analysed the activity of a network of "digital news sites" disseminating pro-Russian content to international audiences.

Initially this network was made up of at least 193 websites covering local news in Russia and Ukraine. It has grown since Russia's invasion of Ukraine in February 2022 and is concentrated in the occupied Ukrainian territories and several Western countries, including France, Germany and Poland, which have shown support for Ukraine.

The websites in this network do not produce any original content but massively relay publications from three types of sources: social media accounts of Russian or pro-Russian actors, Russian news agencies and official websites of local institutions or actors.

The main objective is to cover the Russia-Ukraine conflict presenting Russia's "special military operation" positively and denigrating Ukraine and its leaders. Very ideologically oriented, this content presents grossly inaccurate or misleading narratives that, with regard to the portals targeting France, pravda-fr[.]com, Germany, pravda-de[.]com, and Poland, pravda-pl[.]com, directly contribute to the polarization of public debate.

In order to reach a wider audience, this network uses several techniques, such as the careful selection of pro-Russian propaganda sources according to the targeted location, massive automation in content dissemination, and search-engine optimization.

Conclusion

Converging analysis today shows that public denunciation is one of the main ways to fight information attacks. It involves detecting, characterizing, condemning and widely publicizing such campaigns.

Moreover, our government is working to protect our democracy and our citizens who are directly targeted by these information attacks.

In the case of the RRN and Stars of David manoeuvres, the condemnation of the acts has helped contain the impact of these campaigns.

Russia is using substantial human, financial and technical means to attack France, with so-far limited results. France and its European partners are exercising extreme vigilance and strengthening their coordination.