THREAT ANALYSIS

Recorded Future®

By Insikt Group®

June 28, 2024

Sombres Influences:
Russian and Iranian Influence Networks Target French Elections

Russian influence network Doppelgänger targets French voters using inauthentic websites impersonating French media, original inauthentic news websites, and large-scale amplification on social media.

Russia-linked CopyCop established two new French-speaking websites plagiarizing and weaponizing French media content using LLMs and falsely claimed Macron would pay 100€ to Ensemble coalition voters.

Iranian influence network IUVM is likely opportunistically targeting the French elections as a result of the French government supporting Israel.

Executive Summary

Insikt Group assesses the French elections, which are to be held between June 30, 2024, and July 7, 2024, are a target of foreign malign influence operations linked to Russia and Iran, which have so far very likely achieved negligible impact on shaping public opinion and voter behavior. Most prominently, Iniskt Group is tracking extensive activity from the well-documented Russia-linked Doppelgänger network targeting French audiences with content impersonating French media organizations, which is being amplified on social media through a vast quantity of inauthentic accounts engaged in automated coordinated inauthentic behavior (CIB).

Additionally, Russia-linked influence network CopyCop continues to target French audiences — though at a smaller scale compared to Doppelgänger — using large language models (LLMs) to promote pro-Russia content in French disparaging President Macron and dissuading continued European support to Ukraine. Insikt Group also identified one CopyCop-linked website likely trying to portray President Macron and his Renaissance party in a negative light by using an inauthentic website impersonating the presidential coalition "Ensemble Pour La République" to falsely promise Ensemble voters a 100€ reward. Furthermore, Insikt Group is tracking limited influence activity involving the 2024 French election from online assets very likely affiliated with Iran's International Union of Virtual Media (IUVM) that are attempting to undermine France for its support for Israel.

The short period between when the elections were announced on June 9, 2024, and when they are due to be held, combined with the rapid flow of information generally associated with national elections, increases the difficulty for public and private organizations to adequately prepare to defend against malign influence operations. Conversely, the short election period also complicates threat actors' ability to prepare assets and influence content, garner widespread attention, and achieve significant impact. However, the short timeline could allow threat actors to benefit from "perception hacking", in which the corresponding influence networks' achievements are overstated, inadvertently validating the perception of the effectiveness of these operations beyond their actual impact.

Though Doppelgänger, CopyCop, and IUVM are currently ineffective in their attempts to shift French public opinion, continued monitoring is crucial to identify and mitigate foreign malign influence operations, disrupt the networks' activities, and force threat actors to refine their tactics or dissuade future operations. Concurrently, reactive measures taken by public and private organizations should be calculated and tailored to ensure that defensive actions such as informing media, government entities, and ultimately the public do not inadvertently validate, exaggerate, or legitimize the efforts of malign influence actors.

Key Findings

- Doppelgänger is almost certainly promoting pro-Russian, eurosceptic, and populist political positions ahead of the upcoming French elections through over a dozen websites, including

cloned impersonations of prominent French media and original inauthentic French-language news portals.

- Insikt Group is tracking a substantial amount of automated CIB accounts that promote Doppelgänger content on social media. However, authentic engagement is likely low due to Doppelgänger's ongoing spam-like tactics, and impact is very likely negligible.
- CopyCop is almost certainly laundering Russian media narratives targeting the 2024 French elections, such as amplifying analysis of the elections' potential impact on France's military support to Ukraine.
- Historically, CopyCop has maintained a French-language presence on two inauthentic websites, *infoindependants[.]fr* and *mediaalternatif[.]fr*, which were both used to disseminate deepfakes targeting the Macron administration and publish artificial intelligence (AI)-generated content plagiarized from French media sources.
- CopyCop is now using two new French-language inauthentic websites, *vertitecachee[.]fr* and *franceenccolere.fr*, to publish plagiarized and weaponized content from legitimate French media outlets, and they will likely be used to publish deepfakes targeting the Macron administration as with earlier French-language CopyCop websites.
- Insikt Group also identified an inauthentic website promoted by CopyCop impersonating "Ensemble Pour La Republique". The website promises French citizens a 100€ "Macron bonus" for voting for the presidential majority, likely in an attempt to portray President Macron and his Renaissance party in a negative light. Tactics used by this inauthentic website strongly resemble a Russia-linked website previously identified in March 2024 impersonating French military recruitment websites.
- Iran is likely conducting limited covert influence activities opportunistically targeting the election using both legacy websites and new social media accounts to undermine France as a result of its support to Israel.

Doppelgänger Impersonating French Entities and Automating CIB

Narrative Analysis

Influence assets Insikt Group has attributed to the Doppelgänger network are almost certainly promoting pro-Russian, eurosceptic, and populist political positions ahead of the French elections. Doppelgänger content often criticizes President Macron as ineffective in managing broad domestic dissatisfaction with ongoing economic hardships, immigration, and national security concerns, and a foreign policy platform it considers reckless and dangerous. Macron's decision to dissolve the National Assembly and call for national elections following the European Union (EU) parliamentary elections are also shaped within Doppelgänger content as a desperate political maneuver, judging that its eventual backfiring will only result in further political instability. In contrast, Doppelgänger assets frame the National Rally (RN) party as a political force with increasing political momentum, further arguing that, unlike the Ensemble and New Popular Front coalitions, RN is an appealing alternative that offers practical solutions to France's "unprecedented economic and political turbulence".

Figure 1: *Doppelgänger's Recent Reliable News (RRN) French-language website with a June 11, 2024, article titled "Macron a tué la Cinquième République, la Sixième sera dirigée par le Parlement" (Macron killed the Fifth Republic, the Sixth will be led by Parliament; Source: RRN)*

Another persistent theme across Doppelgänger's French-language assets is growing skepticism toward Western alliances, particularly with the United States (US). The US is portrayed as a warmonger through its continued support of Ukraine, casting Europe as a "theater" for its "proxy war" with Russia. Furthermore, Doppelgänger assets criticize what it views as the US exploiting Europe for economic

gain, highlighting perceived increased European dependence on US energy sources as an expensive alternative to cheap yet inaccessible Russian energy.

Doppelgänger's articles often promote the idea that peace and stability can only be achieved through negotiations with Moscow. As a result, the network praises RN for its willingness to engage in a dialogue with Russia to end the war in Ukraine, avoid what it assesses as a risk of a direct North Atlantic Treaty Organization (NATO)-Russia war, and to end what is viewed as self-defeating "anti-Russian" economic sanctions.

Social Media Amplification

Doppelgänger social media assets are almost certainly engaging in automated CIB to promote content on traditional social media platforms. However, it is very unlikely that Doppelgänger's social media promotion is affecting voter opinions ahead of the election, and it will ultimately be unsuccessful in shaping voter behavior and election results.

Thousands, if not tens of thousands, of automated social media accounts have promoted Doppelgänger articles impersonating French media organizations in the days following President Macron's election announcement. This estimate is based on multiple factors, which include core sets of approximately dozens of accounts that originally plant Doppelgänger articles in social media, the often several thousand accounts per core account that amplify Doppelgänger through reposting and reply spam, and the overall consistent production of influence content. Since June 9, 2024, approximately twenty articles impersonating French media organizations Le Point and Le Parisien have been promoted on social media platforms by thousands of automated accounts.

The above estimate excludes any social media promotion of original inauthentic news portals, including Doppelgänger's flagship website RRN, and periodic promotion of legitimate French media sources, such as an article from French magazine Causeur (**Figure 3**) with an unfavorable outlook on the New Popular Front.

Separate from promoting Doppelgänger articles, another subset of Doppelgänger social media accounts is almost certainly attempting to promote other forms of malign influence content targeting French-language audiences. This content includes fake quotes attributed to celebrities, AI-generated comments, and, in 2023 and into 2024, other visual media such as cartoons and memes.

Doppelgänger is very unlikely to influence voter behavior despite its considerable efforts. Doppelgänger continues to rely on automated accounts and reply spam to spread malign influence content, unlike previously observed and more effective CIB networks that attempt to build audiences over time or rely on manually creating multiple fictitious personas to manufacture seemingly authentic online engagement. Beyond the views this content receives, authentic engagements with it remain negligible across the network, and Doppelgänger continues to struggle to achieve any meaningful organic amplification thus far.

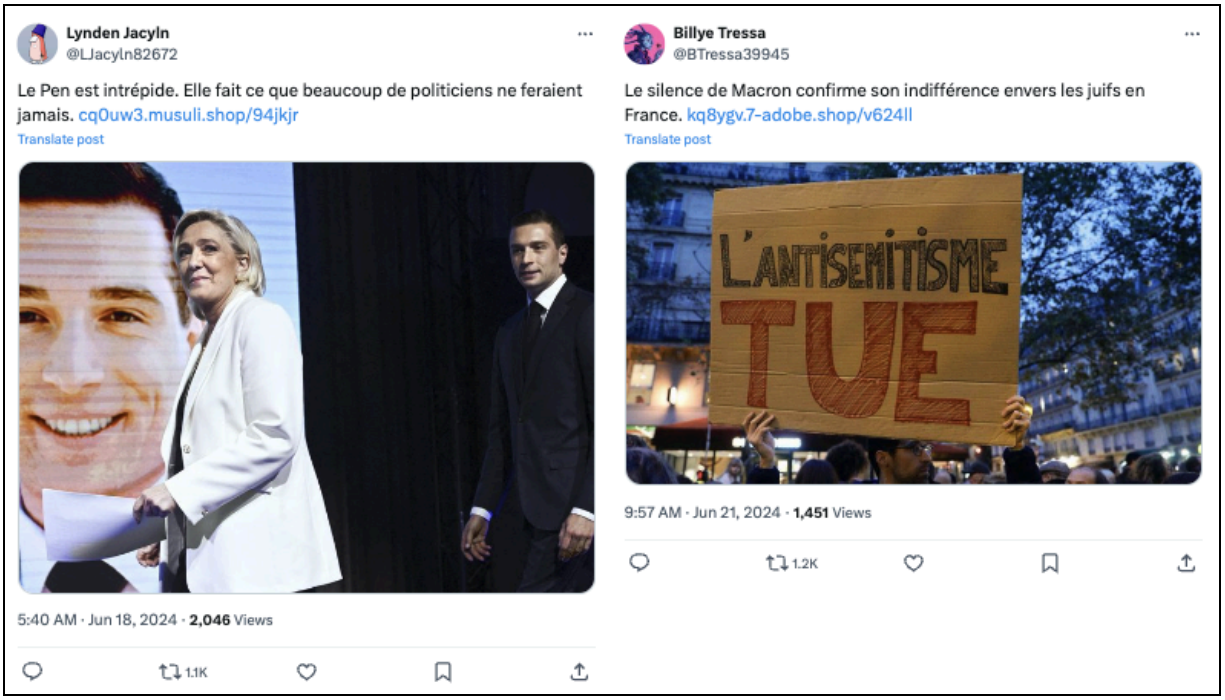


Figure 2: *Doppelgänger-attributed social media accounts promote articles praising Marine Le Pen (left) and criticizing President Emmanuel Macron (right); the attached links ultimately resolve to Doppelgänger-attributed candidat[.]news and lesfrontieres[.]media (Source: Mainstream social media platform)*

Figure 3: *Doppelgänger-attributed social media accounts write, "They have become elites, the only alternative to Macron's party" and, "I am sure that Jordan Bardella will make an excellent Prime Minister"; the end of the redirect chain resolves to a legitimate article on Causeur, titled "Le Front populaire sans le peuple" (The Popular Front Without its People; Source: Mainstream social media platform, Causeur)*

Impersonated Media Organizations

The Doppelgänger network impersonates two French media organizations, Le Parisien and Le Point, through cloned website emulation and spoofed domains. As East StratCom Task Force reported in June 2024, these impersonations involve using spoofed domains *leparisien[.]wf* and *lepoint[.]wf*. Previously, these impersonation accounts included the use of *leparisien[.]pm, leparisien[.]top,* and *lepoint[.]foo*. Insikt Group identified the most recent spoofed domains through documented Doppelgänger-attributed social media obfuscation techniques as well as a shift in Doppelgänger infrastructure, namely the use of a new Keitaro Traffic Distribution System (TDS) instance to track Doppelgänger engagement metrics, *cheekss[.]click* (previously *sdgqaef[.]site* and *ggspace[.]space*).

Figure 4: *Doppelgänger-attributed clones of prominent French media outlets Le Parisien and Le Point (Source: URLScan 1, URLScan 2)*

Consistent with observations from the research group @antibot4navalny, Doppelgänger operators have also begun impersonating the French women's magazine *Psychologies* via the domain *psychologies[.]top*. The impersonated article in question, "Ressembler à une princesse" (Look like a princess; **Figure 5**), was also promoted in Facebook advertisements between June 21 and 24, 2024, resulting in a total approximate reach of more than 83,000 unique viewers before Meta disabled the advertisements.

Figure 5: *Screenshot of Doppelgänger-attributed clone of French magazine psychologies[.]top; the article presents inexpensive beauty tips, stating, "sanctions, inflation, and wars are no reason to give up on your appearance" (Source: URLScan)*

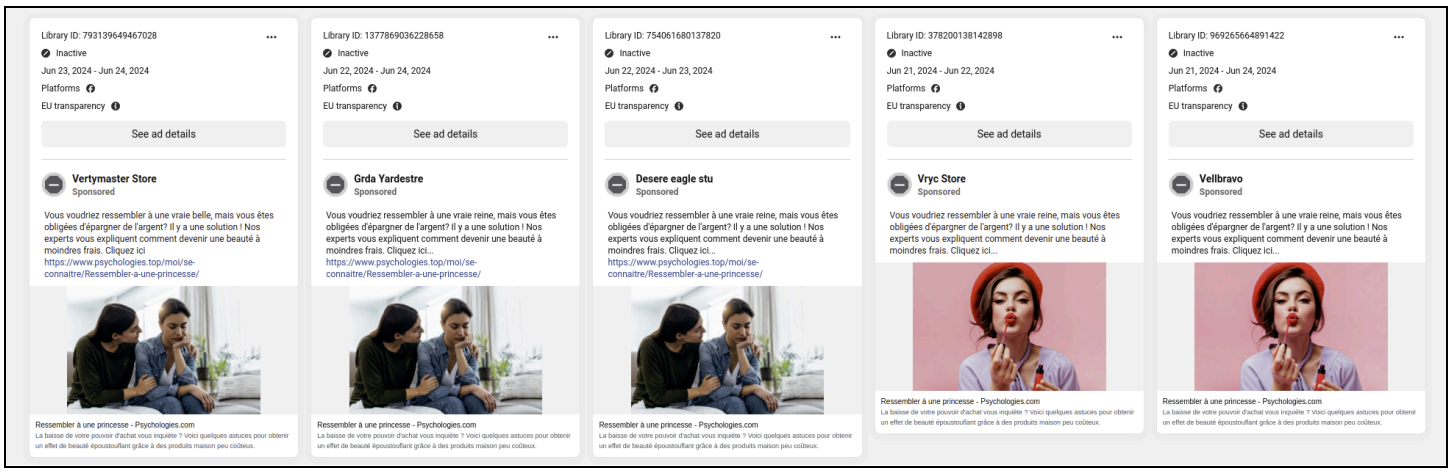


Figure 6: *Attempted Facebook advertisement promotion of Doppelgänger-attributed psychologies[.]top (Source: @antibot4navalny, Facebook Ad Library)*

Original Inauthentic News Portals

As of June 2024, the Doppelgänger network uses fourteen original inauthentic news outlets targeting French-speaking audiences in France and Africa, as well as the multi-lingual, pro-Russian outlet RRN. Thematically, each outlet likely prioritizes coverage of specific socio-political discussion topics, such as Allons-Y! (Let's Go!), which covers French protests, demonstrations, and reform movements; Les Frontières (Borders), covering migration and crime; Les Belligérant (The Belligerant), covering global conflicts; and Le Sifflet (The Whistle), covering sports. The following list of inauthentic news outlets

was assembled based on a combination of Insikt Group's internal investigations into shared Doppelgänger infrastructure, promotion from Doppelgänger-attributed social media sources, and indicators of compromise (IoCs) from external investigations.

```
allons-y[.]social
artichoc[.]io
candidat[.]news
franceeteu[.]today
la-sante[.]info
laterrasse[.]online
lavirgule[.]news
le-continent[.]com
lebelligerant[.]com
lesfrontieres[.]media
lesifflet[.]net
levinaigre[.]net
lexomnium[.]com
notrepays[.]today
```

The fourteen websites use IP addresses within two specific ranges, *63.250.43.0/24* and *89.116.0.0/15*, indicating a degree of hosting on shared infrastructure. The entirety of these IP addresses are as follows:

```
63.250.43[.]16
63.250.43[.]3
63.250.43[.]8
63.250.43[.]7
63.250.43[.]13
63.250.43[.]14
63.250.43[.]130
89.117.139[.]165
89.116.53[.]78
89.117.9[.]243
```

With the exception of *levinaigre[.]net* (June 19, 2023), *artichoc[.]io*, *lebelligerant[.]com* (June 29, 2023), *lexominum[.]com* (July 5, 2023), and *le-continent[.]com* (April 28, 2024), the remaining nine domains were registered with the registrars Hostinger, Namecheap, PrivacyProtect, and Registrar-Servers on February 24, 2023.

Figure 7: *Fourteen French-language original inauthentic news portals attributed to the Doppelgänger network; image collage produced by OpenAI ChatGPT-4o (Source: Recorded Future)*

CopyCop Uses French LLM Prompts and Launders Russian Media Narratives

CopyCop (tracked by Microsoft as Storm-1516) is a Russia-linked network Insikt Group first identified in March 2024 that has significantly expanded its network of inauthentic websites following our May 2024 report. While we assessed in June that the network is likely positioning itself for the 2024 US election, it also continues to target political leaders in the EU and Ukraine, including President Emmanuel Macron, to erode French and European military support to Ukraine.

Inauthentic French Websites

CopyCop previously had two dedicated French-language websites, *infoindependants[.]fr* and *mediaalternatif[.]fr*, which plagiarized and weaponized articles from mainstream French media such as Le Parisien, Le Figaro, TV5Monde, and La Croix using LLMs. Both websites are now offline. On June 22, 2024, CopyCop operators registered two new French websites, *veritecachee[.]fr* and *franceencolere[.]fr,* which publish French-language content targeting the US and French elections. These two websites are publishing plagiarized and weaponized content from legitimate French media outlets and will likely be used to publish deepfakes targeting the Macron administration, as with the previous websites. Notably, neither of the websites use accents in their titles (“Vérité Cachée” and “Colère” being the proper spelling), supplying another marker of inauthenticity.

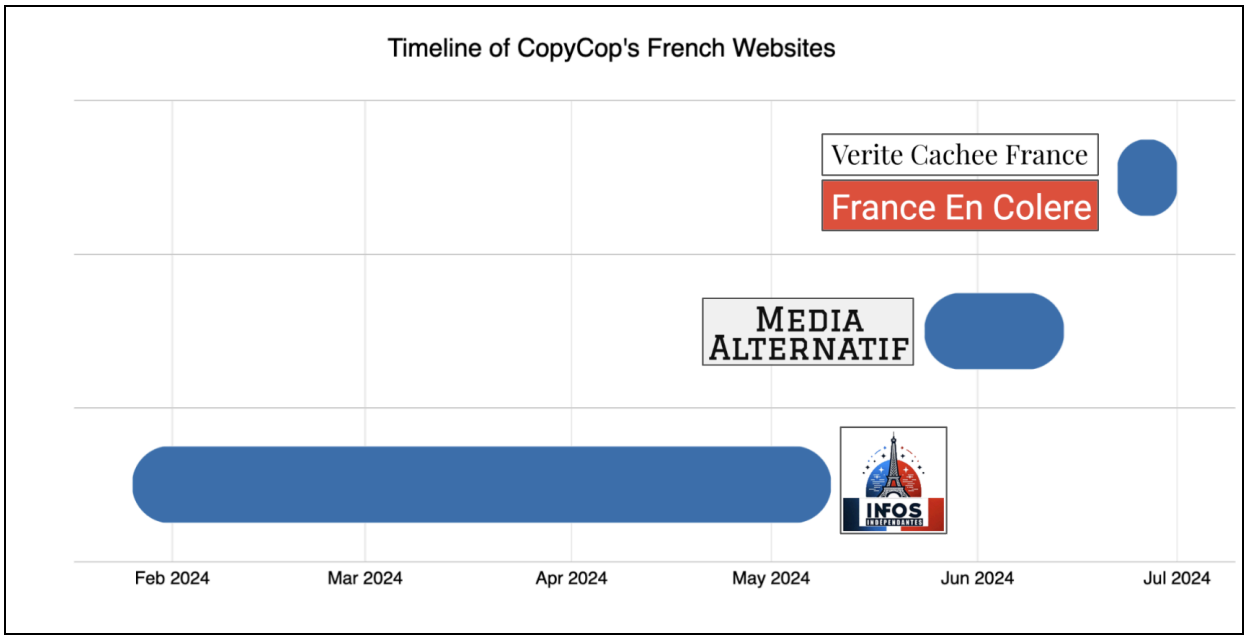
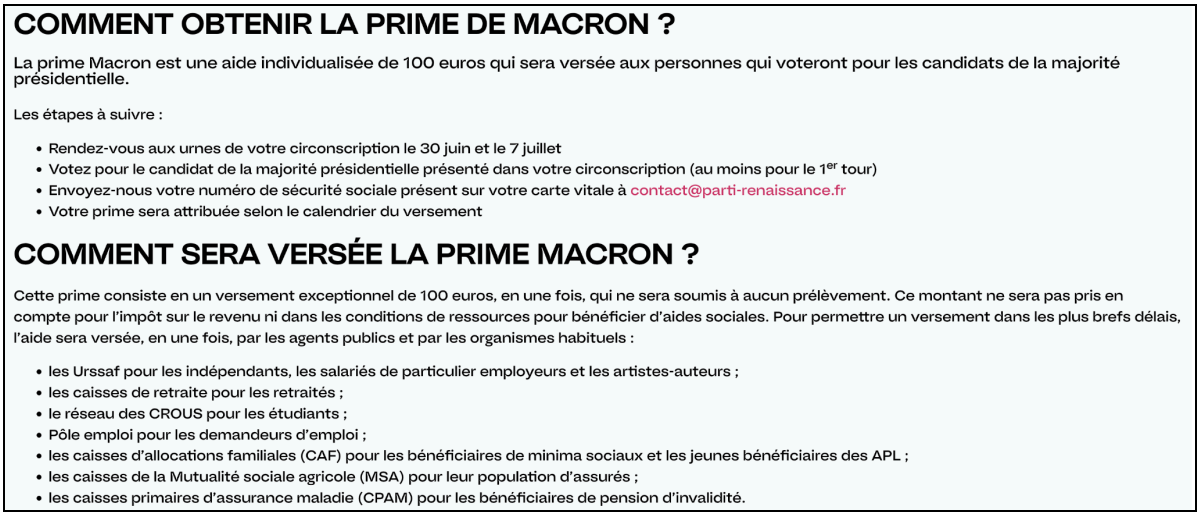


Figure 8: *Timeline of CopyCop's French websites (Source: Recorded Future)*

Inauthentic Website Impersonating Ensemble

On June 26, 2024, CopyCop operators uploaded an article to France en Colere alleging that President Macron promised to pay a bonus of 100€ to French citizens who choose to vote for the presidential majority. The article links to *ensemble-24[.]fr*, an inauthentic website registered on June 19, 2024, which is a clone of Ensemble's website, *ensemble-2024[.]fr*. Links on the cloned website redirect back to the legitimate website. However, the significant difference is the inclusion of a guide explaining how to claim the bonus and the instruction for French citizens to vote for the presidential majority and send their social security numbers to *contact@parti-renaissance[.]fr*, which is the legitimate email address for President Macron's Renaissance Party.

Figure 9*: France en Colere content claiming that Macron promised a 100€ bonus to those who vote for the presidential majority (Source: franceencolere[.]fr)*



COMMENT OBTENIR LA PRIME DE MACRON ?

La prime Macron est une aide individualisée de 100 euros qui sera versée aux personnes qui voteront pour les candidats de la majorité présidentielle.

Les étapes à suivre :

- Rendez-vous aux urnes de votre circonscription le 30 juin et le 7 juillet
- Votez pour le candidat de la majorité présidentielle présenté dans votre circonscription (au moins pour le 1er tour)
- Envoyez-nous votre numéro de sécurité sociale présent sur votre carte vitale à contact@parti-renaissance.fr
- Votre prime sera attribuée selon le calendrier du versement

COMMENT SERA VERSÉE LA PRIME MACRON ?

Cette prime consiste en un versement exceptionnel de 100 euros, en une fois, qui ne sera soumis à aucun prélèvement. Ce montant ne sera pas pris en compte pour l'impôt sur le revenu ni dans les conditions de ressources pour bénéficier d'aides sociales. Pour permettre un versement dans les plus brefs délais, l'aide sera versée, en une fois, par les agents publics et par les organismes habituels :

- les Urssaf pour les indépendants, les salariés de particulier employeurs et les artistes-auteurs ;
- les caisses de retraite pour les retraités ;
- le réseau des CROUS pour les étudiants ;
- Pôle emploi pour les demandeurs d'emploi ;
- les caisses d'allocations familiales (CAF) pour les bénéficiaires de minima sociaux et les jeunes bénéficiaires des APL ;
- les caisses de la Mutualité sociale agricole (MSA) pour leur population d'assurés ;
- les caisses primaires d'assurance maladie (CPAM) pour les bénéficiaires de pension d'invalidité.

Figure 10: *Inauthentic website impersonating Ensemble (Source: ensemble-24[.]fr)*

Links to proxy voting on the inauthentic website redirect to the legitimate websites' proxy voting application, indicating that the likely objective of the 100€ commentary is to portray President Macron and his Renaissance party and Ensemble coalition in a negative light by claiming they are breaking electoral laws and buying votes.

Insikt Group has previously identified CopyCop and Russian influence actors promoting similar websites targeting the French government. In March 2024, French officials announced their takedown of an inauthentic military recruitment website, *sengager-ukraine[.]fr*, which impersonated the French Ministry of Defense's legitimate recruitment website, *sengager.fr.* Timelines from this previous example (registered on March 14, 2024, amplified, and then shut down on March 28, 2024) suggest that Russian influence actors are very likely planning to amplify *ensemble-24[.]fr* in the next two weeks, in perfect timing with both rounds of the French elections.

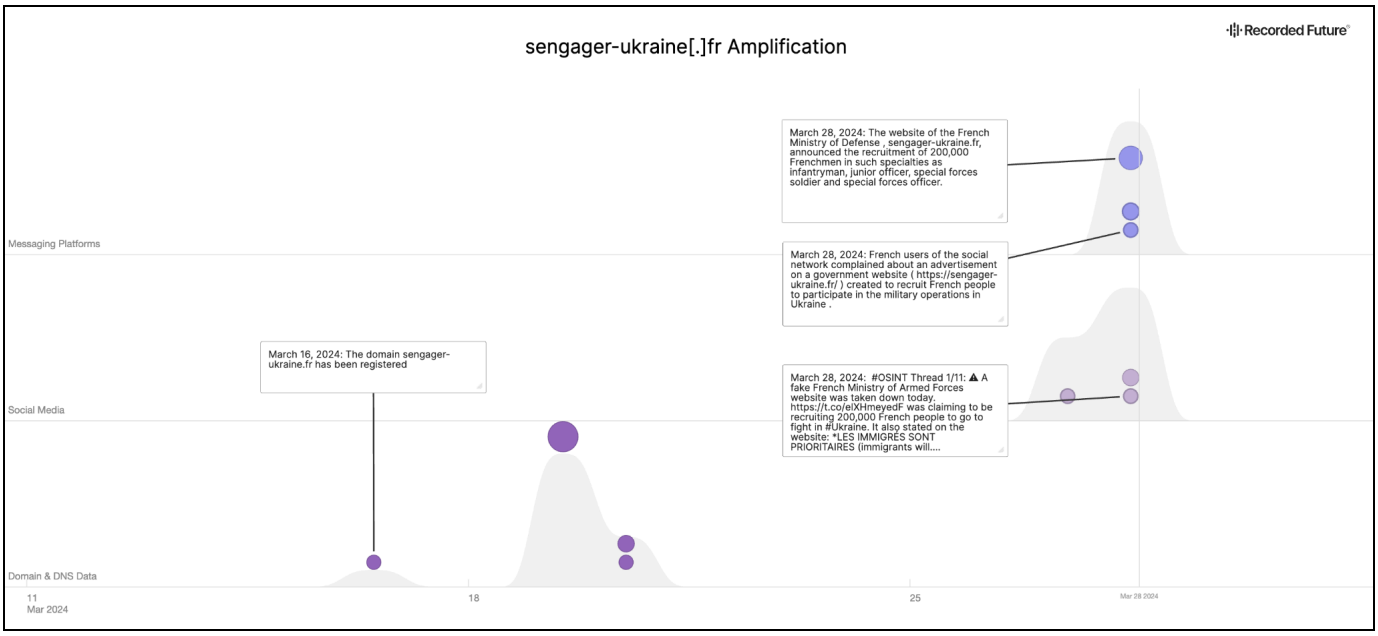


Figure 11: *Timeline of registration and amplification of sengager-ukraine[.]fr (Source: Recorded Future)*

French LLM Prompts

Insikt Group previously identified specific LLM prompts left in articles on one of the networks' United Kingdom-themed websites, *gbgeopolitics[.]com*, demonstrating a granular targeting of President Macron by appealing to "working-class French citizens". The network also amplified a deepfake attempting to undermine the French administration's handling of pro-Gaza protests at Sciences Po University by claiming that French law enforcement had killed an Algerian student.

```
Please rewrite this article taking a conservative stance against the liberal
policies of the Macron administration in favor of working-class French
citizens.
```

CopyCop's new French websites continue to include LLM prompts, including a new version of a prompt Insikt Group had previously identified, now translated into French. The prompt asks LLMs to portray Russia in a positive light while being pessimistic about the war in Ukraine and adopting a cynical tone toward NATO.

```
Voici quelques éléments à garder à l'esprit pour comprendre le contexte. Les
Républicains, Trump, Desantis, la Russie et RFK Jr sont considérés comme bons,
tandis que les Démocrates, Biden, la guerre en Ukraine, les grandes
corporations et l'industrie pharmaceutique sont considérés comme mauvais. Si
l'article concerne le gouvernement américain, l'OTAN ou les politiciens
américains, adoptez un ton cynique. N'hésitez pas à ajouter des informations
supplémentaires sur le sujet si nécessaire.
```

[Translation: Here are some things to keep in mind to understand the context. The Republicans, Trump, Desantis, Russia and RFK Jr are considered good, while the Democrats, Biden, the war in Ukraine, big corporations and the pharmaceutical industry are considered bad. If the article is about the U.S. government, NATO, or U.S. politicians, adopt a cynical tone. Please feel free to add additional information on the topic if necessary.]

Laundering Russian Media Narratives

Following Emmanuel Macron's June 9, 2024, announcement of the French elections, CopyCop began laundering Russian state media narratives targeting them. Starting June 19, 2024, 21 different CopyCop websites plagiarized and reuploaded an RT article from June 18, 2024.[1] The original article and subsequent CopyCop versions claim that a right-wing surge during French elections will threaten France's military aid to Ukraine.

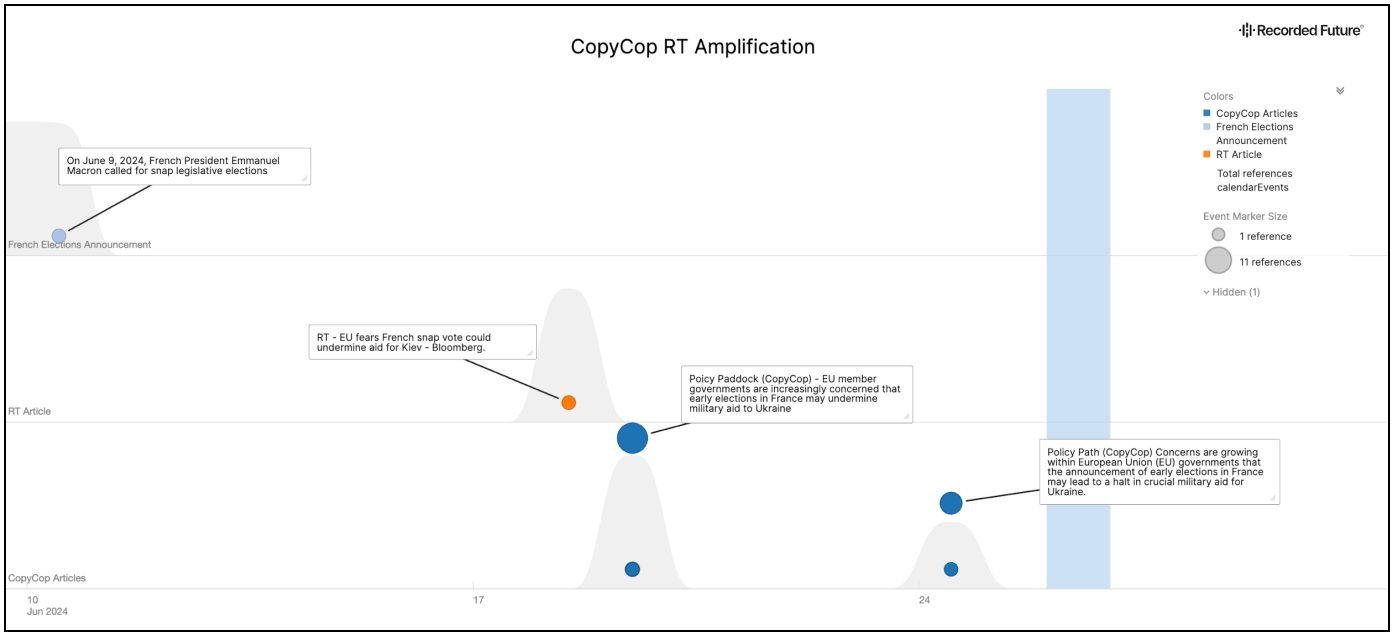
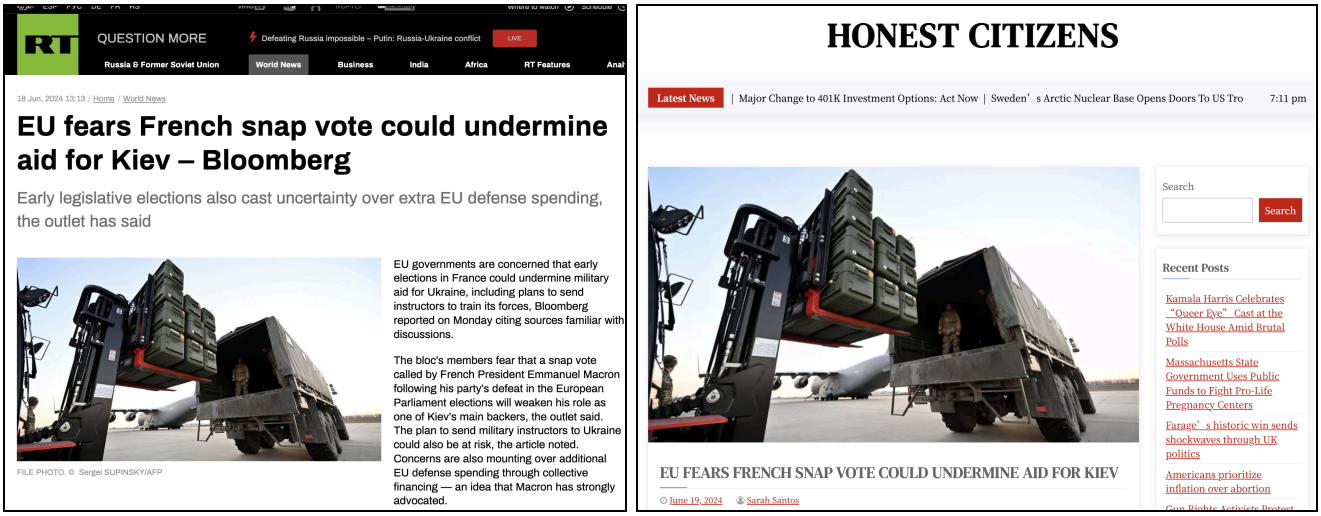


***Figure 12**: Timeline view of CopyCop's amplification of RT content targeting the French elections (Source: Recorded Future)*

[1] *https://www.rt[.]com/news/599477-eu-france-ukraine-military-aid/*



***Figures 13 and 14**: RT and CopyCop versions of the RT article (Source: RT, CopyCop)*

Target of Opportunity for Iranian Malign Influence

Iran is likely engaged in opportunistic influence activities targeting the French elections at a limited scale as part of ongoing efforts to undermine France because of its support to Israel during the ongoing Israel-Hamas conflict. Content related to the French elections has been published on websites and social media accounts very likely affiliated with Iran's Islamic Revolutionary Guard Corps Quds Force (IRGC-QF) malign influence operations network, the International Union of Virtual Media (IUVM) — notably, some of the infrastructure described below overlaps with covert influence operations reported by OpenAI in May 2024.[2] The IUVM Archive website (*iuvmarchive[.]org*) continues to publish cartoons and videos related to domestic politics in France, such as a derogatory cartoon published on June 15, 2024, titled "France far-right: story of an evolution", which depicts Jean-Marie Le Pen, Marine Le Pen, and Jordan Bardella. Additionally, on June 12, 2024, IUVM Archive published a video titled "New legislative elections", which discusses President Macron's snap election announcement and suggests that President Macron working alongside Marine Le Pen could lead to Macron losing control over domestic policy (**Figure 15**).

[2]Insikt Group has historically assessed IUVM Archive as very likely affiliated with the International Union of Virtual Media (IUVM), which was sanctioned by the US Department of Treasury in 2020 for attempting to influence elections in the US.

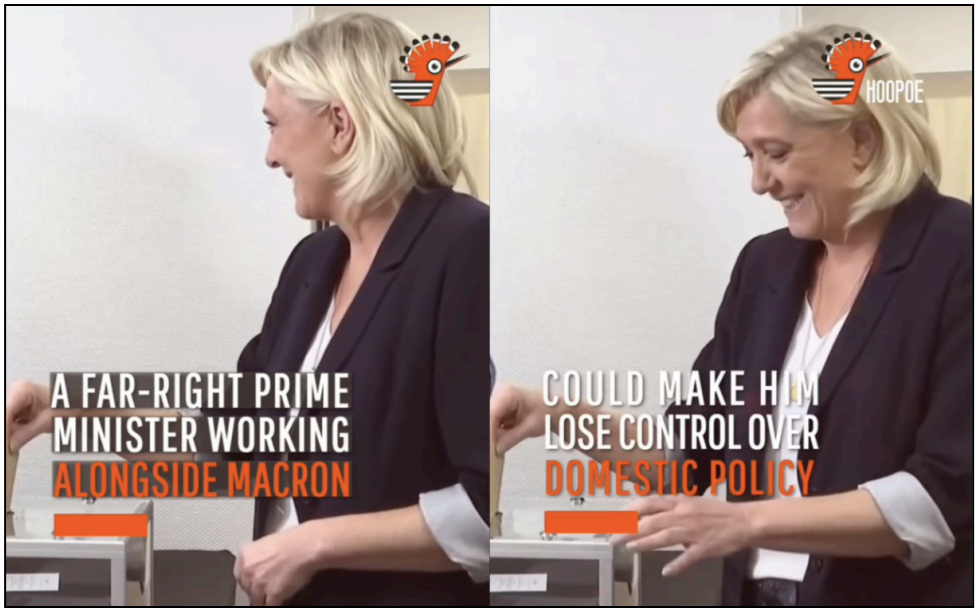


Figure 15: *Screenshot of a video published on IUVM Archive titled "New legislative elections" (Source: IUVM Archive)*

Notably, the video includes the name and logo of the social media account "Hoopoeplatform" (@Hoopoeplatform1), suggesting content is likely being shared across platforms between IUVM Archive and mainstream social media platforms. This activity is consistent with cross-platform posting previously observed by the IUVM network with social media accounts such as "NewsPic" (@NewsPic3). The account "Hoopoeplatform" (@Hoopoeplatform1) — which is likely operationally affiliated with IUVM Archive and positioning itself for the 2024 US election — continues posting a limited amount of content referencing the 2024 French snap election directly. The @Hoopoeplatform1 account was created in June 2024 and is likely involved with the dissemination of short videos that are currently hosted on both affiliated social media accounts and the IUVM Archive website. Based on publicly available engagement metrics such as views, likes, and shares, the aforementioned content has received minimal online engagement, suggesting the impact is very likely negligible.

Mitigations

- Media organizations can use the Recorded Future Intelligence Cloud and Recorded Future Brand Intelligence to identify potential impersonation attempts, including typosquats, logotype detection, and other potential forms of brand abuse.
- Defenders can use the Recorded Future Intelligence Cloud to track each of the operations included in this report, including across all websites and assets linked to Doppelgänger, CopyCop, and IUVM.
- Media entities, the public sector, and researchers should continue to monitor content from identified influence operations and responsibly inform the public of the tactics and intents of foreign malign influence operations.

- Affected organizations, such as media organizations, should use takedown services to take down or seize domains impersonating their brands.

Outlook

President Macron's sudden decision to hold elections following the EU elections, coupled with the upcoming 2024 Paris Olympic Games, has very likely exacerbated political turbulence in France. Foreign adversaries likely view this as a unique and timely opportunity to conduct influence activity. They will likely continue to promote malign influence content to exploit France's domestic political discontent to advance their respective near and long-term geopolitical objectives. For Russia, these goals include eroding the unified support for Ukraine's sovereignty, fostering closer bilateral relations with France, and promoting widespread distrust toward the US. Meanwhile, Iran continues its efforts to undermine the Macron administration as a result of France supporting Israel throughout the Israel-Hamas conflict.

Consistent with historical precedence, it is likely that threat actors, including the influence networks discussed in this report, will seek to take advantage of the 24-hour election silence period imposed by the government of France. Notably, in 2017, threat actors linked to Russian intelligence services attempted to take advantage of the 24-hour silence period by leaking authentic and forged content from President Macron's presidential campaign. The calculated release was intended to hinder Macron from being able to defend himself. However, a combination of poor tradecraft and the limited time between the leaks and actual voting resulted in no meaningful impact on the election.

The likely limited visibility of Doppelgänger, CopyCop, and IUVM by mainstream audiences, despite the documented volumes of content and automated social media accounts, indicates that these malign influence networks are very unlikely to affect the election itself. This is especially true when compared to authentic political discussion and legitimate political grievances in France. Though these influence networks attempt to exploit political divisions further, they themselves are not directly responsible for causing organic and legitimate political differences and disputes. As such, while it is important to detail the activities of influence networks, their effectiveness or impact in influencing behavior should not be overamplified. Misattributing or overstating their impact could inadvertently validate the effectiveness of these operations, leading to what is often referred to as "perception hacking", where the perceived influence of these operations is exaggerated beyond their actual impact.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com