Lessons from Paris 2024: Toward a Coordinated and Future-Proof European Strategy Against FIMI

Léo le Douarec

December 2025

Executive summary

France was arguably well prepared to face Foreign Information Manipulation and Interference (FIMI) threats, and managed to mitigate most of the attempts surrounding the 2024 Paris Olympics. The multiplicity of attacks and methods employed required the implication of cross-disciplinary and cross-sectorial skills ranging from technical, political, and physical capabilities.

VIGINUM, France's organization focusing FIMI at the national level, underlined the importance of civil society, pre-bunking and de-bunking, and cautious risk-assessment before denouncing information campaigns. It noticed that most disinformation during the Olympics remained restricted to first-publishers and detected hybrid methods combining cybersecurity attacks with Foreign Digital Interference (FDI) operations [14].

Through examples surrounding the Paris 2024 Olympics, this essay proposes a reflexion on possible cooperation mechanisms, as well as future threats in the information warfare. This essay argues that although France effectively mitigated most FIMI threats during the Olympics, the event revealed pitfalls in EU-level cooperation, particularly in cybersecurity-FIMI integration, social media platforms' accountability, and techno-legal coordination. We list certain recommendations, stating that the EU should:

- Foster cross-sectoral and interdisciplinary cooperation. It should tie together cybersecurity and FIMI mitigation, as examples (such as ANSSI and Billboard hacking [22] of cyberwarfare in Georgia [29]) show this is an increasingly topical issue.
- Create mechanisms for techno-legal cooperation between institutions through platforms such as PeReN or the Maastricht Law and Tech Lab on technical topics such as social media monitoring under the DSA, and Article 50 of the AI Act [28].
- Involve social media platforms and create incentives for them to willingly cooperate with state institutions (e.g. VIGINUM), sharing quality data to more accurately detect, monitor and document inauthentic behavior online.
- The EU AI act should be at the center of Europe's legislative battle against inauthentic, AI-generated content online, by fully implementing the recommendations that will come out of the public consultation on transparency and article 50 of the legislation.
- Finally, the EU should officially recognize the threat of hybrid warfare in countries such as Georgia, Moldova, and others being targeted by Russia. This is a first step to ensure credibility of EU foreign policy, recognizing the shift of Russia from a failed direct war in Ukraine to hybrid threats in neighboring countries [29].

Table of Contents

Definition of terms and methodological choices

This essay's methodological approach is based on the analysis of concrete examples that help understand policy implications at national and European levels. It focuses on the Paris 2024 Olympics but also draws from other relevant examples when useful.

This essay will focus on **disinformation**, since it tackles information campaigns that aim to *deliberately create harm, manipulate or mislead* [33]. Since the operations are conducted in the digital world with the objective to undermine France's democratic values and electoral processes, we will mostly talk of FIMI and FDI as defined by the European External Action Service (EEAS) and VIGINUM.

We will also use the concept of *Hybrid Warfare*, defined by the EEAS as the use of a mix of measures to exploit vulnerabilities of a state, while remaining below the threshold of formal warfare [2]). In this essay, we will also underline the fact that hybrid attacks sometimes involved the hacking of physical systems (e.g. advertisement billboards) to disseminate false information, instead of relying solely on fake accounts and social media.

Introduction

In April 2025, France officially denounced Russia's continuous disinformation operations and cyber attacks against the country across the years: TV5Monde (2015), MacronLeaks (2017), French presence in Africa (2020), RRN campaign (2023), Paris Olympics (2024) to name only a few. This announcement is a first, strong diplomatic symbol of the tensions between the two countries, and the scale of Russia's attempts to disrupt France's cyberspace [1].

Indeed, France has long been a target of FIMI from foreign national actors such as Russia, China, Iran or Azerbaïdjan [14], even though Russia has been the most prominent and long-standing one. The attack on TV5Monde was the first hybrid[1] attack in France [3] - disrupting service for a few hours and taking control of the TV network's social media accounts with messages supporting ISIS. It was followed 2 years later by the leaking of emails and document of Emmanuel Macron's campaign, just hours before the 2-day blackout period prior to the elections. Both these interferences aimed at disturbing public debate, creating fear or disorientation in the mind of the french people. These actions use democracies' greatest asset as a fatal flaw: the free flow of information, supposed to reinforce democracy, becomes its pitfall by allowing the propagation of manipulated speech, documents, and facts.

Following these events, France has been a leading country in the field of tackling FIMI and related cybersecurity issues, leading the 2018 ”Paris call” urging signatories to fight against foreign electoral manipulations, and creating VIGINUM in 2021. This pioneering approach inspired the EU in the wake of the elections in Romania, Moldova and Slovakia for example. After the creation of Stratcomm in 2015, a task force aiming to tackle FIMI and strategic communication at the European level through portals such as EUvsDisinfo [4], the European commission recently presented the European Democracy Shield, coordinating national agencies such as VIGINUM at the european level [32].

Social media and the internet are key platforms for the mass dissemination and amplification of fake and manipulated news [5]. This means that legislation in this sector - namely the DSA, the GDPR, and the AI Act - must be at the center of the stage when talking about safety of the digital public debate.

[1] Hybrid warfare in general is the use of a mix of measures to exploit vulnerabilities of a state, while remaining below the threshold of formal warfare [2]). Here, we also underline the fact that it involved the hacking of the system to disseminate false information, instead of just disseminating information through fake accounts.

With the digital space as a new battlefield, the companies managing these platforms hold power and thus, responsibility through their moderation policies and the data they accept to share with authorities.

Considering this context, his essay will tackle the following question: **what insights do the Paris 2024 Olympics bring for the current and future fight against FIMI** ? And to what extent can existing cooperation mechanisms be enhanced ? This essay argues that although France effectively mitigated most FIMI threats during the Paris 2024 Olympics, the event revealed pitfalls in EU-level cooperation, particularly in cybersecurity-FIMI integration, social media platforms' accountability, and techno-legal coordination.

We will first examine the ecosystem focused on preventing FIMI operations during the Paris 2024 olympics. We will then present the aftermath of the olympics, analyzing what actors, narratives and modus operandi were seen during the games and what it means for FIMI mitigation. In the light of these insights, we will analyze the levers at the disposal of policy makers to better fight disinformation, focusing on European cooperation and future threats such as AI-powered disinformation campaigns.

I - France's strategy to fight FIMI during the Paris Olympics

I.1 France's doctrine on FIMI

> Our adversaries have no limits. We fix ourselves a lot of boundaries
>
> *A. Bonnemaison, director of COMCYBER [3]*

France's doctrine regarding FIMI is defensive, much like its wider doctrine regarding cyber warfare. Similarly to the latter, it is also ill-defined. ANSSI[2] ex-director Patrick Pailloux sums up France's cybersecurity doctrine as follows: "when we have to chose between protecting our country and putting it in danger, we always chose to protect it" [3], even if the recent law on military planning [6] plans to take a more offensive stance. The decision ultimately comes to the highest officials in the most sensitive matters.

The creation of VIGINUM in 2021 proves France's defensive doctrine regarding FIMI (contrary to Russia's weaponization of disinformation in Europe). The organization's sole purpose is to monitor FIMI and protect France against them. As one of the first agencies of this type in Europe, it pushes for cooperation between national and private actors to build a resilient digital public space [7]. For example, VIGINUM is at the origin of many open source tools that are being tested and used by other governments in the European Union, such as detection tools of AI-generated content [8]. It also pushed to harmonize practices between multiple actors with the OpenCTI initiative.

Contrary to other countries such as Russia, France refrains from conducting offensive influence operations in other countries. As summed up by A. Bonnemaison, director of the french comcyber, *"our adversaries have no limits. We fix ourselves a lot of boundaries."* [3]. A telling example is France's strategy to counter Wagner's operation on French interests in Africa (Françafrique). In 2020, in Mali and the Central African Republic, France (more precisely the French army's COMCYBER) decided to create bot accounts that denounced Russian disinformation online [3], [9]. The accounts

[2] Agence Nationale de la Sécurité des Systèmes Informatiques, France's cybersecurity agency.

did not impersonate anyone, and did not disseminate fake news - they only tried to counter Wagner's disinformation efforts at undermining France's already fragile reputation in the area.

Even this defensive approach has been criticized, particularly in the case of Françafrique, with researchers claiming that using fake accounts to pass on messages on social media further fragilizes the digital public space, and ”implicitly justifies the behaviours that [the french authorities] are trying to fight” [3], [10].

I.2 Analysis of the French ecosystem to fight FIMI prior to the olympics

VIGINUM is not the only agency tackling FIMI and FDI in France. In this paragraph, I will briefly draw a sketch of the French ecosystem that was in place to counter disinformation during the olympics.

The Paris 2024 Olympics was an event that concentrated special attention from all around a world, and were as such a perfect opportunity for foreign actors that wanted to destabilize french public debate and its international image. In 2024, French authorities already had some experience with FIMI, as explained in the introduction. Precedent Olympic games had also seen major attacks [11], [12]. The organizers thus announced an investment of 350 million euros in security (including fighting disinformation campaigns) [13] and collaborated with cybersecurity firms such as Cisco and Eviden, while VIGINUM started monitoring social media as early as April 2023 [14].

The main body coordinating the answer to cyber-related threats at the national level is the SGDSN[3]. This service reports directly to the french prime minister and serves as an administrative body for agencies such as VIGINUM, the Interministerial Control Group (GIC), and the ANSSI. The SGDSN coordinates these agencies and assists the prime minister in decision making and legislative drafting in areas related to national defense and security. ANSSI also coordinates with other intelligence agencies whose activities are linked to VIGINUM's, inside the ”Center for coordination of cyber crises”[4] [15],[16],[17]. Figure 1 summarizes the relationships between these entities.

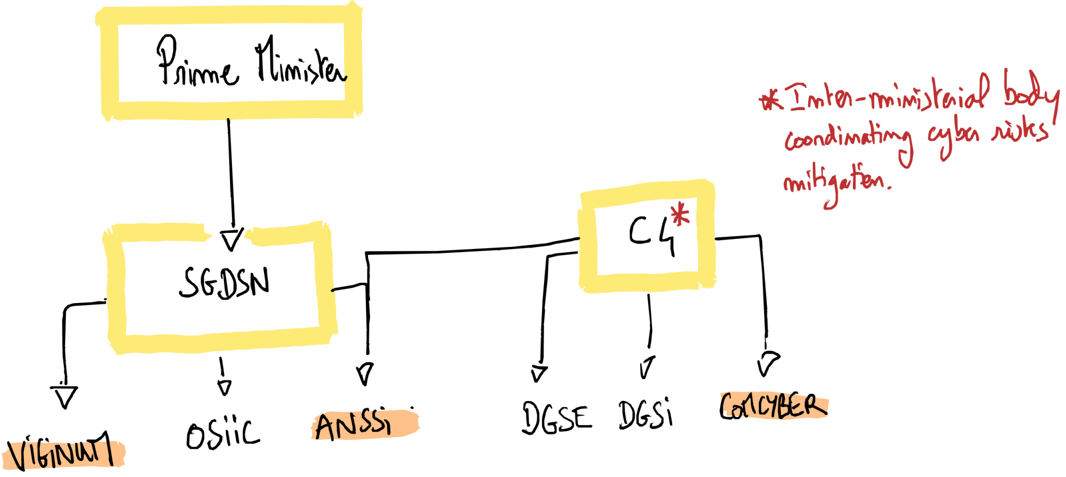
Prime Minister
SGDSN
C4*
*Inter-ministerial body coordinating cyber risks mitigation.
VIGINUM
OSIIC
ANSSI
DGSE
DGSI
COMCYBER

Figure 1: Main institutional organizations involved in FIMI are highlighted in Orange. Sources: [15],[16],[17]

During the Olympics, VIGINUM remained at the center of investigations and surveillance of online discourse in France, and has coordinated multiple actors in anticipation of the olympics - while ANSSI

[3] Secrétariat Général de la Défense et de la Sécurité Nationale - General Secretariat for National Defense and Security

[4] Also known as the ”C4”.

also held a critical line of defense since some disinformation attempts were coupled with cyber attacks. For example, it published guides for economic actors [18], as well as for media and fact-checkers [19] . Indeed, news media played a key role in pre-bunking and de-bunking online disinformation, such as Radio France [20] or Les Échos [21].

However, VIGINUM also relied on a network of international partners that contributed to identifying threats, vulnerabilities, and malevolent actors. This is the case of Microsoft's Threat Analsyis Centre (MTAC) who identified 2 Russian-aligned actors (Storm-1679 and Storm-1099) in June 2023, aiming to discredit the Olympics and create a climate of violence during the event [12]. Alphabet's subsidiary Mandiant also published a report in June 2024 warning of high risks of information operations surrounding the olympics, with Russia being the most serious threat [11]. Private actors such as cybersecurity companies (Cisco, Atos) and companies specialized in analysis of social media and Business intelligence (ArlequinAI, Suadeo Hypervision) also complete this private ecosystem.

But GAFAMs and private actors are not the only actors providing insights on FIMI around the olympics. There was also institutional cooperation between allied governments. For example, on July 25th 2024, ANSSI was informed that a company responsible of managing advertisement billboards had been compromised. The FBI warned ANSSI that the attack was operated by an Iranian company that was planning to display modified images to denounce Israeli athletes. This cooperation allowed ANSSI to mitigate the threat, preventing any impact on the games [22].

We thus see that a strong international and cross-sectorial cooperation ecosystem was well-prepared to counter FIMI during the Olympics. The next part will focus on the effectiveness of this organization.

II - Aftermath of the olympics: analysis of the results

In a report [14] published right after the olympics, VIGINUM documented the results of its monitoring, allowing us to analyze the different actors involved in disinformation around the olympics, as well as the methods they used.

II.1 Identified actors

During its monitoring period, VIGINUM detected 43 FDI. Some of them were part of 2 coordinated digital campaigns - one from Azerbaïdjan (codenamed OLIMPIYA), the other from Russia (using methods reminiscent of Matriochka and RRN). Other foreign narratives included deepfakes and influencer videos targeting Mandarin-speaking audiences, as well as pro-Iranian accounts doxxing Israeli athletes [14].

II.2 Narratives

Even if most FDI were conducted on an opportunistic basis, analysis reveals some recurrent narratives, often linked to specific national actors. The main objectives of these narratives were to discredit the capacity of France to organize the olympic games, foster fear in the minds of french people and tourists, and promote different political models than the French one. [14]].

Most notably, some operations by Russia exaggerated existing security concerns (linked to terrorism and immigration, issues that were already well present in the french public debate), as well as the overall cleanliness of Paris (with attacks on pollution of the River Seine [30], as well as amplification of news on bedbugs in October 2023 [23]), arguably targeting hesitant tourists concerned about safety and cleanliness in France.

Additionally, some Russian falsified documents and videos allegedly from France24, AFP, or INSEE[5] reported mass booking cancellations a few days before the opening ceremony, perhaps trying to reduce participation to the event [24] .

Another rather consistent narrative from foreign actors was the doxxing campaign against Israeli athletes participating in the Olympic games in the context of the war between Israël and Hamas (backed by Iran). In parallel, as evoked earlier, a firm from Iran tried - unsuccessfully - to hack into advertisement billboards to display modified photos representing Israeli athletes [22]. Fake news surrounding alleged - but fake - threats of terrorist attacks by Hamas also aimed to fuel fear over security during the olympics.

The narratives being employed by foreign actors, in particular Russia, are not new. In fact, Russia's method is to push forward already-existing narratives and create misleading content to blur the boundary between truth and lie. The objective is to destabilize public discourse in any way possible. But what methods have been used during to accomplish this goal ?

II.3 Modus operandi of foreign actors

Many different methods were used and are rigorously reported by VIGINUM [14]. Some methods used were hybrid, meaning that malevolent actions combined physical attacks with online disinformation narratives, such as the hacking a company managing advertisement billboards, or the ”Cyber Army of Russia Reborn”'s threats of attacking the Parisian water sanitation system in parallel to the Russian Matriochka online campaign discrediting the water quality of the river Seine [30]. Another quite effective hybrid operation involved Moldovan citizens who tagged stars of David referring to the Münich Olympics terror attacks [25]. Photos of these tags were then relayed by accounts known to be related to Russia's RRN FIMI operation [14]

Other methods relied on online platforms and social media-based techniques, with fake accounts being created for astroturfing, creating hashtags (such as #JOpourris2024 or #BloodyOlympics), taking videos out of their context, creating synthetic videos from scratch, or impersonating official media such as AFP, France24 and others like Russia with its Matriochka campaign [14].

In parallel, a rather disturbing way to increase the reach of disinformation content online has been the use of paid influencers. One of the most prominent case during the 2024 olympics was a video published by a 2.4 million subscribers Chinese influencer criticizing the olympics and the opening ceremony in Chinese, which got 2 million views [14].

However, analysts from Google [11] deemed that France was well prepared and benefited from the experience of past olympic games. Subsequently, most of these measures did not permeate to the wider public debate. Most disinformation content remained blocked to ”first-publishers”, unless they were republished by reknowned french public figures, like it was the case regarding a video impersonating Hamas. VIGINUM attributes the little success of these disinformation campaigns to the effective mobilisation of media and civil society [14]. These findings revealpitfalls in France's FIMI defence, which informs the next section on the levers available to policymakers at the french and European levels.

[5] French National Institute for Statistics

III - Lessons from the Olympics to tackle disinformation

We have seen that disinformation campaigns relentlessly destabilize our democracies in Europe, with a focus on major events such as elections or the organization of the olympics. I would like to conclude this policy paper by thinking about the institutional and cross-disciplinary interactions between member states, the EU, private actors and civil society that shape the way we, as Europe, fight disinformation.

III.1 From france to Europe: Cooperation at the European level

France has launched a strong push towards institutionalizing FDI mitigation since the Honfleur Task Force (2020) which led to the creation of VIGINUM (2021). At the European level, the EEAS has long been active in producing common frameworks and initiatives to tackle FIMI, such as

- Analytical tools: FIMI Exposure Matrix (introduced in 3rd EEAS report on FIMI).
- Cooperation tools: Stratcomm and EUvsDisinfo, EDMO[6], European Democracy Shield.
- Legislative tools: Media freedom act, DSA, GDPR, AI Act.

The most recent development in EU policy surrounding FIMI is the presentation in November 2025 of the European Democracy Shield [32]. This initiative aims to provide a platform to foster cooperation between the EU and member states, with Russia's relentless attacks in mind. This platform includes support to fact checkers (via EDMO), collaboration on techniques to monitor disinformation (fostering cooperation with agencies such as VIGINUM and Stratcomm) and legislative backing under the Digital Services Act (DSA). This confirms the role of Europe as a regulatory, policy and monetary support to fight disinformation in a coordinated way.

III.2 What is missing from current cooperation mechanisms ?

The existing cooperation frameworks at the national (french) level and European level are already strong, and are bound to become even stronger with the EU Democratic Shield. However, we argue that 3 main approaches remain under-used to ensure a fully efficient answer to the growing threats from Russia (and to a certain extent, China as seen during the 2024 olympics).

III.2.1 Cybersecurity and FIMI

As seen during the olympics, some of the most dangerous and effective FDIs were the result of a hybridation of economic, political, technical and psychological methods [14], for example combining fake accounts and cybersecurity breaches. Current cybersecurity and FIMI governance frameworks (such as the French C4 and Stratcomm) should thus include inter-sectoral coordination to ensure that actors exchange information and methods to prevent FIMI operations. In the context of the EU, this means the ENISA, EDMO and Stratcomm need to have a dedicated exchange platform to coordinate.

[6] European Digital Media Observatory

III.2.2 Social networks

Social networks are at the core of the FDI since they host the content that citizens interact with. They thus have access to data that is central to monitor unauthentic information online, yet they are quite distant from discussions on FDI. This is where the EU's Digital Services Act (DSA) is a critical instrument. Most popular social networks qualify as ”Very Large Online Platforms” (VLOPs) and thus are subject to stringent obligations - including external risk auditing and data-sharing requirements [31]. However, VIGINUM officials recognized that they do not really cooperate with social media platforms. They only discuss about strategies, without real framework or incentive for platforms to cooperate[7].

Consequently, there seems to be some room for improvement, all the more so as platforms such as X have been failing short of their obligations regarding data sharing since Elon Musk's takeover. In this context, the concept of Data Intermediaries introduced by the DSA could be used to put in place a concrete structure whose aim would be to centralize social network data for monitoring purposes by VIGINUM or similar agencies. This however raises important questions of surveillance and privacy even though it is legal under the GDPR and the DSA: one could criticize such a measure as an attempt to infringe on individual rights by making it easier for governments to monitor behaviours online. This is where VIGINUM's approach to publish aggregated results is important, and safeguards should be put in place to ensure that this approach remains respectful of privacy.

III.2.3 Techno-Legal cooperation

Additionally, we see that topics relating to Data and AI are increasingly technical while having some strong legal and social ramifications. Institutions bridging technical and legal expertise on highly technical topics such as PerEN in France or the Maastricht Law and Tech Lab could serve as examples for broader techno-legal cooperation. The EU's JRC could serve as a platform to foster these exchanges between scholars and government.

III.3 Future threats

Europe and its allies are facing major threats as of today due to misinformation and hybrid warfare. What is looming at the horizon, and how can we best prepare for it ?

III.3.1 AI-powered disinformation

Traditional disinformation already impacts different countries with many different methods, as seen in figure 2. The rise of AI is a serious and short-term threat that will bring disinformation to a whole other scale; with massively generated text, images and videos, creating disinformation is becoming easier. Regulatory instruments like the AI Act are critical to adressing the issue of generative AI (genAI) in disinformation. In particular, article 50 of this piece of legislation requires transparency measures from providers of genAI models, and a public consultation ended in October 2025 to help the EU decide on which practical mechanisms could be implemented to be able to detect generated content online. Cooperation between LLM builders (e.g. OpenAI) and governments will be critical to efficiently detect and take down operations that use LLMs to generate misleading content, such as the *Helgoland Bite* operation identified by OpenAI in a June 2025 report [26].

[7] This last point was discussed during an intervention of a VIGINUM official during one of my classes

For example, watermarking [34] could be a promising way to implement the provisions of article 50 [28]. However, one must keep in mind that watermarking is not yet fully ready to be deployed at scale. In fact, one of the main pitfalls of current watermarking techniques is that they could be replicated by malevolent actors - for example, if someone knew what watermark OpenAI uses, then they would be able to create text that mimics ChatGPT, opening a door to false claims of illegal content produced by ChatGPT - which is not in the interest of OpenAI and undermines the original objective of being able to detect text generated by an LLM.

In addition, there is growing concern over genAIs becoming skewed due to manipulation of their training data. For example, NewsGuard found that the Pravda network[8] was built as an effort to influence web crawlers and genAI to have them output skewed content, rather than directly influencing people.

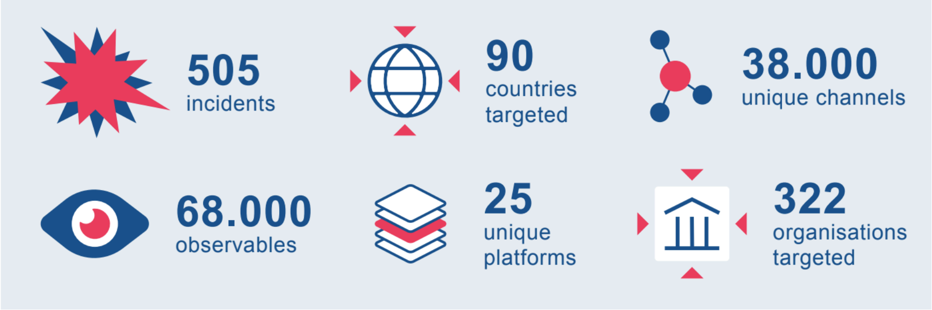

Figure 2: Source: 3rd EEAS report on FIMI.

Conclusion: uncertainty and Russia's strategy in Europe

> How do you fight totalitarianism with democratic means ?
>
> *Salomé Zourabichvili, current president of Georgia [29]*

The Paris 2024 Olympics are an example of a robust and mostly successful FIMI monitoring by the French state and its international partners. While the French framework was satisfactory, it could be further enhanced by improving techno-legal cooperation, involving social media in stronger cooperation with state actors, and blending more closely cybersecurity and FDI monitoring.

With the US's ambiguity towards Europe and Russia, the EU is in a difficult and uncertain position. In March 2025, the USA announced stopping their cyber-operations against Russia, a surprise for Europe, with all the implications for the cooperation with Ukraine on the battlefield and in the cyberspace [27].

In the mean time, seeing strong resistance on the Ukrainian battlefield, Russia seems to be redirecting its efforts to hybrid warfare, as pointed out by the current Georgian president. Georgia is, according to Salomé Zourabichvili, a test ground for Russia and should be at the heart of Europe's preoccupations. One year ago, the country was on track to become a fully-fledged EU Member state, but this process has been abruptly stopped and since then, the country has fallen under a spiral of Russian influence,

[8] A network of approximately 150 false information portals published in multiple languages

combining information warfare, cyber attacks and remote political control. Elections in Romania, Moldova are other examples of the shift in Russia's strategy.

Among all this uncertainty, one thing is certain: Russia is implementing a large-scale strategy to undermine European and allied democracies, with limited military involvement. But "how do you fight totalitarianism with democratic means ?" [29]. This paper has shown that effective cross-border and cross-sectoral collaboration is critical to exchange knowledge, and ensure relevant data is available to the relevant actors, while preserving privacy online. The EU has the legislative levers, and the technical means, to implement a union-wide counter-strategy. With an evidence-based and systematic monitoring of FIMI attempts, it could be able to mitigate threats.

Word count: 4116 (automatically counted by Overleaf).

Disclosure - Use of generative AI: This essay was written from the ground up without using generative AI. The only use of generative AI was to copy-paste the instructions of the teachers in a prompt to proof-read the essay and get a second opinion on the title. If interested, one can read the discussion with the LLMs by clicking on the following links:

- ChatGPT conversation
- Claude conversation

I have put a lot of time and consideration into writing this essay and would be very thankful to have detailed, thoughtful feedback from your end in order to improve my writing and thinking. I respectfully ask you to refrain from using fully automated grading, and I expect the same level of transparency on the potential use of AI by the corrector.

References

[1] Ricard, Philippe, and Martin Untersinger. La France Attribue Pour La Première Fois Officiellement Des Cyberattaques à La Russie. Le Monde, 29 Apr. 2025. 4

[2] "Hybrid Threats." Defence-Industry-Space.ec.europa.eu 4

[3] Untersinger, Martin. Espionner, Mentir, Détruire. Grasset & Fasquelle, 2024. 4, 5, 6

[4] ""Stratcom", La "Task Force" Européenne Pour Lutter Contre Les Ingérences Étrangères et La Désinformation En Li." Franceinfo, 4 June 2024 4

[5] Chavalarias, David. Toxic Data. Editions Flammarion, 22 Feb. 2025. 4

[6] "Pour Une Coordination de La Cyberdéfense plus Offensive Dans La Loi de Programmation Militaire 2024-2030 - Sénat." Sénat, 2019. 5

[7] "Service de Vigilance et de Protection Contre Les Ingérences Numériques Étrangères (Viginum) | Choisir Le Service Public." Choisir Le Service Public, 2021. 5

[8] "VIGINUM." GitHub, 15 Sept. 2025. 5

[9] "Removing Coordinated Inauthentic Behavior from France and Russia." Meta, 15 Dec. 2020. 5

[10] More-Troll Kombat - French and Russian Influence Operations Go Head to Head Targeting Audiences in Africa. Graphika, Stanford Internet Observatory, 15 Dec. 2020. 6

[11] Phishing for Gold: Cyber Threats Facing the 2024 Paris Olympics. Mandiant, 5 June 2024. 6, 7, 8

[12] "Tentative de Perturbation Des Jeux Olympiques de Paris 2024 Par La Russie | Security Insider." Microsoft, 2024. 6, 7

[13] "JOP Paris 2024 : Et Si Les Hackers Entraient En Jeu ?" CCI - Chambre de Commerce et D'industrie, 2024. 6

[14] VIGINUM. "Synthèse de La Menace Informationnelle Ayant Visé Les Jeux Olympiques et Paralympiques de Paris 2024 | SGDSN." SGDSN, 13 Sept. 2024. 2, 4, 6, 7, 8, 9

[15] Ministère de l'intérieur. La DGSI Au Cœur de l'Organisation Française de Cyberdéfense | Direction Générale de La Sécurité Intérieure. 2023. 6

[16] SGDSN. Service de Vigilance et Protection Contre Les Ingérences Numériques Étrangères. 6

[17] Sénat. Projet de Loi de Finances Pour 2024 : Direction de l'Action Du Gouvernement : Coordination Du Travail Gouvernemental - Sénat. 2019. 6

[18] SGDSN. Publication d'Un Guide de Sensibilisation à La Menace Informationnelle à Destination de l'Écosystème Des Acteurs Économiques Associés Aux JOP24 | SGDSN. 2024. 7

[19] VIGINUM. Foreign Information Manipulation and Interference (FIMI) Threat Awareness Guide for Media and Fact-Checkers during the Olympic and Paralympic Games. July 2024. 7

[20] Radio France. "JO de Paris 2024 : 14 Fausses Informations Largement Relayées Dans Le Monde, Selon Newsguard." Franceinfo, 24 July 2024. 7

[21] Les Echos. JO de Paris 2024 : La Russie Étend Sa Stratégie de Désinformation. 4 June 2024. 7

[22] CERT - ANSSI. Panorama de La Cybermenace 2024. 2, 7, 8

[23] Le Monde with AFP. Bedbug Panic Was Stoked by Russia, Says France. 1 Mar. 2024. 7

[24] NewsGuard. 2024 Paris Olympics Misinformation Tracking Center. 8

[25] Tellier, Maxime. "Étoiles de David Taguées à Paris : L'opération Était Orchestrée Par Des Réseaux Russes." France Inter, 26 Jan. 2024. 8

[26] OpenAI. Disrupting Malicious Uses of AI: June 2025. 10

[27] Parmentier, Audrey. "Etats-Unis : Pourquoi Le Pentagone Met En Pause Ses Cyberopérations Contre La Russie." L'Express, 3 Mar. 2025. 11

[28] Rijsbosch, Bram, et al. "Adoption of Watermarking for Generative AI Systems in Practice and Implications under the New EU AI Act." ArXiv.org. Maastricht Law and Tech Lab, 2025 2, 11

[29] Sciences Po. 60 Minutes with Salomé Zourabichvili, Fifth President of Georgia | Sciences Po Alumni. 2023. 2, 11, 12

[30] Barnes, Julian E. "Unable to Penetrate Systems, Hackers Spread Lies about Vulnerabilities." The New York Times, 3 Oct. 2024. 7, 8

[31] *VLOPs are subject to stringent obligations including external risk auditing and data-sharing requirements*. Course "Fake News, Disinformation and Foreign Digital Interference: Key Challenges For the Future of the EU. 10

[32] Lemaître, Camille. "Pour Lutter Contre La Désinformation, l'UE Planche Sur Un "Viginum Européen."" Geo.fr, 12 Nov. 2025. 4, 9

[33] *Disinformation is deliberately created to harm, manipulate, or mislead*. Course "Fake News, Disinformation and Foreign Digital Interference: Key Challenges For the Future of the EU. 4

[34] Kirchenbauer, John, et al. "A Watermark for Large Language Models." Proceedings.mlr.press, PMLR, 3 July 2023. 11