

Health Disinformation: A New Tool for Foreign Interference

How health became a target of information warfare

- Foreign Information Manipulation and Interference (FIMI) often seeks to stoke polarisation and divisions inside and outside the EU while also aiming to undermine the EU's global standing and ability to pursue its policy objectives and interests.¹
- Modelling suggests that online mis- and dis-information can drive infection peaks up to six times higher during a pandemic.²
- In two years, Storm-1516, a Russian information network, has carried out more than 150 information manipulation operations.³

Information has become a weapon. Short of armed conflict, foreign powers are running coordinated disinformation campaigns to sway public opinion, undermine democratic institutions and deepen social divisions. NATO considers such information-based threats a risk to national security and an integral part of hybrid warfare strategies.⁴ In fact, Kaja Kallas, EU High Representative for Foreign Affairs and Security Policy and Vice-President of the European Commission, has said "*Today's wars are not only fought with tanks and drones but with lies and algorithms too.*"⁵

For several years now, the EU has been one of the main targets of foreign interference, particularly from Russia and China. FIMI has been recognised as an increasing security and foreign policy threat for the EU, with the European External Action Service (EEAS) playing a key role in the EU's response. Through FIMI, foreign powers are stepping up their digital campaigns to influence public opinion.

Health holds a special place in this new information war. Since the COVID-19 pandemic in particular, treatments, vaccines and scientific expertise have been repeatedly attacked. False claims have circulated about the virus' origin, the effectiveness of treatments and the safety of vaccines, while media outlets have been impersonated, influencers approached and conspiracy theories amplified at large scale.

¹ [Information Integrity and Countering Foreign Information Manipulation & Interference \(FIMI\) | EEAS](#)

² [Matthew R. Verena and al., « Modeling the amplification of epidemic spread by individuals exposed to misinformation », NPJ Complexity, 02 avril 2025](#)

³ [Stratégie nationale de lutte contre les manipulations de l'information d'origine étrangères, 2026-2030](#)

⁴ [OTAN, Lutte contre les menaces hybrides](#) et [Approche de l'OTAN pour la lutte contre les menaces informationnelles](#).

⁵ [4th EEAS Report on Foreign Information Manipulation and Interference Threats](#)

Yet these campaigns do not necessarily aim to convince citizens of a particular medical theory. Their goal may be broader: to exploit health fears and uncertainties in order to sow mistrust, deepen social divisions and weaken a state's ability to make collective decisions and win public acceptance for them. Health thus becomes an entry point for attacking something highly strategic: trust in institutions. It is therefore the defence of our democratic systems that is at stake.

WHY HEALTH REMAINS A PRIME TARGET FOR MANIPULATION

From private fear to collective vulnerability

Why has health become such fertile ground for interference?

The answer lies first and foremost in its place in our lives. Health affects everyone, either directly or through loved ones. An illness, an epidemic, a vaccine or a new treatment can cause real concern, and in these moments of uncertainty, information becomes particularly sensitive.

According to the European Commission, the COVID-19 pandemic was accompanied by an "avalanche of false or misleading information and attempts at foreign influence on national debates within the EU," which exploited "the fertile ground of citizens' most primal fears and the rapid pace of information."⁶

However, the end of the COVID-19 crisis has not put an end to the infodemic, nor to foreign interference in health matters.

Several features make health an especially attractive topic for disinformation campaigns. Firstly, it affects the entire population, guaranteeing a broad audience. Secondly, it deals with highly emotional topics, which tend to go viral on social media. Finally, it relies on trust: in scientists, healthcare professionals, the media and the institutions responsible for protecting the public. This combination makes it a particularly effective target.

A vulnerability further amplified by digital platforms

Social media further reinforces this vulnerability. According to one study, accurate information takes about six times longer than false information to reach users.⁷ Algorithms favour attention-grabbing content, which gives sensational or anxiety-inducing content a built-in advantage.

⁶ [Commission Européenne, 10 juin 2020, Lutter contre la désinformation concernant la Covid-19: "Démêler le vrai du faux"](#)

⁷ [Les Echos, 11 mars 2018, Pourquoi les fake news se propagent bien plus vite](#)

In just a few months in 2021, more than 100 new cases of pro-Kremlin disinformation about vaccination were added to the EUvsDisinfo⁸ database. At the time, the European External Action Service (EEAS) assessed that these campaigns were part of a "vaccine diplomacy" strategy, combining promotion of the Russian vaccine with disinformation aimed at undermining trust in Western vaccines, European institutions and the EU's vaccination strategies.⁹

Health is thus a prime target for foreign interference because it allows influence over both individual behaviour and collective trust. It is this very trust that FIMI campaigns are targeting.

WAR THROUGH OTHER MEANS: THE INFORMATION FRONT

Coordinated attacks tailored to current affairs

Information manipulation for the purposes of foreign interference is not new, but its scale, speed and sophistication have changed profoundly.

The EU defines Foreign Information Manipulation and Interference (FIMI) as "a set of behaviours, most of which are not illegal, that threaten or are likely to have a negative impact on values, procedures and political processes."¹⁰ These activities are deliberate and coordinated. **They generally seek to fuel polarisation and division within European societies, while undermining their political interests and international standing¹¹.**

New digital tools give the perpetrators of these campaigns an unprecedented capacity to act. They can produce content at massive scale, target specific audiences, react almost instantly to current events and repeat the same narrative in different forms.

At EU level, the EEAS has been working on countering FIMI since 2015¹². Building on this work, the Commission proposed a European Democracy Shield package in 2025. This also saw the establishment of a Special Committee on the European Democracy Shield in the European Parliament.

The current EEAS' strategy to counter FIMI has three mutually reinforcing pillars¹³:

1. faster responses, thanks to improved data and operational coordination
2. scaled up cooperation with partners, strengthening joint capabilities

⁸ [Covid-19 Disinformation, EEAS special report](#)

⁹ Ibid

¹⁰ [European Union External Action](#)

¹¹ Ibid.

¹² [Carriages preview | Legislative Train Schedule](#)

¹³ [4th EEAS Report on Foreign Information Manipulation and Interference Threats](#)

3. greater impact, by shifting from reaction to anticipation and disrupting the infrastructures and incentives that sustain FIMI

Despite these efforts to strengthen the EU's response, recent campaigns illustrate how FIMI continues to evolve and how these tactics are being used to spread disinformation across Europe and the EU. Several recent campaigns from 2025 illustrate this new form of information-based conflict:

- Operation Doppelganger, for instance, impersonated legitimate media outlets, for ex. French media outlets *Le Monde* and *20 Minutes* to create fake pages and disseminate fake articles.¹⁴
- Operation Matryoshka, which played a part in disseminating false information about the spread of the hantavirus in France.¹⁵
- Storm-1516 (also known as CopyCop or False Façade), for its part, disseminates false audiovisual content in a coordinated manner, designed to infiltrate authentic public discourse¹⁶

These operations share a common feature: they no longer rely solely on the dissemination of isolated pieces of false information. They seek to construct an information environment in which it becomes increasingly difficult to distinguish truth from falsehood. Public health is fully integrated into this new strategy.

FROM COVID-19 TO MICROBIOLOGICAL LABORATORIES

When health becomes a geopolitical tool

The use of health-related disinformation in foreign campaigns is not new. As early as 2018, a study of Russia-linked accounts on Twitter found that they were amplifying false information about vaccines in order to undermine public consensus on vaccination.¹⁷

These campaigns intensified during the COVID-19 pandemic, which became a battleground for a full-scale information war. Vaccines, treatments and the origins of the virus were at the centre of numerous campaigns. EUvsDisinfo, in particular, documented how the Kremlin disseminated disinformation and conspiracy theories in several languages, insinuating that "elites" were using the virus for their own ends.¹⁸ **The aim was to foster mistrust of national authorities and scientific institutions.**

¹⁴ [Le Monde, 13 juin 2023, Révélation sur Doppelganger, la campagne de désinformation russe dénoncée par la France](#)

¹⁵ [NewsGuard's Reality Check, 20 mai 2026, Hantavirus Is Overrunning France \(According to Russia\)](#)

¹⁶ [4th EEAS Report on Foreign Information Manipulation and Interference Threats](#)

¹⁷ [AJPH, Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate](#)

¹⁸ [EuvsDisinfo, EEAS SPECIAL REPORT: Disinformation on the coronavirus – short assessment of the information environment, 19 mars 2021](#)

Some campaigns have also sought to enlist influencers to reach audiences directly on social media. In one case, French influencers were approached by an unidentified communications agency offering large sums of money to spread content discrediting the Pfizer-BioNTech COVID-19 vaccine. They were instructed in particular to claim that the vaccine was responsible for more than a thousand deaths worldwide, without disclosing that the video was sponsored.¹⁹ The origin of this attempt at destabilisation has not been established, although links to Russia have been suspected.²⁰

The war in Ukraine then showed how health issues could be integrated directly into a geopolitical strategy.

Since Russia's invasion of Ukraine in 2022, the Kremlin has accused the United States and Ukraine of operating laboratories on Ukrainian territory to produce biological weapons. According to this narrative, a network of some 30 laboratories allegedly carried out dangerous experiments and stored disease strains such as the plague or cholera, in collaboration with the US Department of Defense.²¹ EUvsDisinfo has since documented dozens of variations on this narrative. More recently, a pro-Kremlin disinformation campaign accused the United Kingdom of sending drones to Kyiv carrying mosquitoes infected with modified pathogens such as Zika or malaria.²²

The approach is always the same: turning a health issue into a geopolitical narrative. Research facilities are cast as suspect, scientists as participants in an alleged conspiracy, viruses as weapons, and Western authorities as a threat.

Health thus becomes a tool for fuelling division and even confrontation. **The goal is not always to make people believe something; it is to sow doubt.**

This may be one of the most troubling aspects of these campaigns. A FIMI operation does not necessarily need to convince the public to adopt a specific opinion. It can be effective simply by sowing enough confusion and mistrust to cast suspicion on any information from official sources.

The study "*Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate*" illustrates this particularly well. Examining tweets about vaccination between 2014 and 2017, the authors identified significant activity from Russia-linked accounts, but these accounts did not all take the same side: some messages were pro-vaccine, others anti-vaccine.²³ This contradiction was not a weakness of the strategy but,

¹⁹ [Le Monde, 24 mai 2021, Des youtubeurs français incités à dénigrer le vaccin contre le Covid-19 de Pfizer-BioNTech](#)

²⁰ [Courrier international, 26 mai 2021, Des influenceurs français approchés pour dénigrer le vaccin Pfizer, la Russie soupçonnée](#)

²¹ [Le Monde, 12 mars 2022, Guerre en Ukraine : la propagande russe sur les armes biologiques inquiète les Occidentaux](#)

²² [EUvsDisinfo, The UK is moving specialised aircraft to Kyiv to spread mosquitoes infected with modified viruses](#)

²³ [AJPH, Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate](#)

in all likelihood, its very core. The aim was not to promote a single position on vaccines but to exacerbate divisions already present in society.

This mechanism aligns with a concept well documented in science communication research: "science-related populism", as conceptualised by Mede and Schäfer²⁴. The framework describes a set of beliefs that pit "ordinary people", endowed with common sense, against "academic elites" seen as dishonest, out of touch or serving hidden interests. This is not an outright rejection of science as such, but a challenge to the legitimacy of those who produce it. That is why these campaigns do not need scientifically coherent content to be effective: their target is not a medical claim but the authority of the source making it. This is fertile ground for FIMI operations, which supply a ready-made narrative to feed mistrust already latent among a segment of the population.

Health is thus "weaponised": used to promote discord and, ultimately, to undermine people's trust in their institutions. The strategy is particularly effective in societies that are already divided. It does not need to create opposition from scratch; it simply identifies divisive issues, amplifies them, multiplies conflicting narratives and makes each side feel that the other poses a threat. The primary objective, then, is not public health. It is political.

When defiance threatens public health

The consequences of these campaigns, however, are not confined to the online sphere. **Dis-information can change behaviour, delay care-seeking, reduce compliance with preventive measures and complicate authorities' response to a crisis.**

In just a few months in 2020, false information about COVID-19 was linked to thousands of hospitalisations and hundreds of deaths.²⁵ The costs can also be economic: people who turn to ineffective or dangerous treatments drive up healthcare spending. In the United States, for example, 15 people ingested disinfectant in an attempt to protect themselves against the coronavirus.²⁶

A recent study has also shown that, **in certain scenarios, dis-information could raise the peak of an epidemic by up to six times**, notably by undermining adherence to preventive measures.²⁷

²⁴ [Niels G. Mede and Mike S. Schafer, « Science-related populism : Conceptualizing populist demands toward science », Sage Journal, 9 juin 2020](#)

²⁵ [Md Saiful Islam and al, « Covid-19-Related Infodemic and its Impact on Public Health : A Global Media Analysis », The American Journal of Tropical Medicine and Hygiene.](#)

²⁶ [Maria Mercedes Ferreira Caceres and al, « The impact of misinformation on the Covid-19 pandemic », National Library of Medicine, 2022.](#)

²⁷ [Matthew R. Verena and al, « Modeling the amplification of epidemic spread by individuals exposed to misinformation », NPJ Complexity, 02 avril 2025](#)

FROM HEALTH TO DEMOCRACY

A threat on another scale

Interference campaigns do not stop at the boundaries of public health. They can exploit narratives on conflicts, elections, identity issues and public health at the same time, with the aim of destabilising the targeted countries. During and after the COVID-19 pandemic, some MEPs such as Barry Andrews (Ireland, Renew Europe), were the victims of targeted disinformation: accused of being “*the same as the Nazis issuing papers to Jews in the 1930s*” for having voted in favour of the Digital Green Certificate²⁸.

This convergence matters. A single operation can exploit several vulnerabilities at once: health offers a way into people's private lives, elections a way into democratic debate, and conflicts a way to exploit geopolitical fears and identity issues, deepening social divisions. The goal is to spread mistrust from one issue to another. A person who doubts a vaccine does not necessarily doubt democracy. But if they are gradually exposed to content that casts doubt on scientists, doctors, the media, health authorities and then political institutions, a much deeper conclusion may take hold: that no one can be trusted. The OECD notes that foreign interference can affect sovereignty, trust, economic growth and security.²⁹

Trust: a democratic infrastructure under threat

Health-related disinformation should no longer be seen as merely a communication issue. It is not just a handful of false posts circulating on social media. It can become an instrument of strategic confrontation, exploiting a society's vulnerabilities and weakening its ability to respond collectively to crises.

In a FIMI operation, health is the entry point, trust is the target, and democratic resilience is what is at stake. Protecting the public from health disinformation is therefore not only a matter of debunking false information once it has spread. It also means safeguarding the conditions that allow a society to withstand a crisis: reliable information, credible institutions, independent science and a population able to tell fact from manipulation.

Health has become a new front in the information war. It is time to treat it as one.

²⁸ [Disinformation and Covid](#)

²⁹ [OCDE, 22 avril 2024, Renforcer la transparence et l'intégrité des activités d'influence étrangère en France. Un outil pour lutter contre les risques d'ingérences étrangères](#)

CONTACTS

Elise Rodriguez, Deputy Director
erodriguez@ghadvocates.org

Rowan Dunn, EU Advocacy Coordinator
rdunn@ghadvocates.org

Fanny Vesse, Advocacy Officer
fvesse@ghadvocates.org