

Combating foreign interference in elections

Although it has always existed, foreign interference in election processes has become increasingly prevalent, exacerbated by new technologies and widespread social media use and increased geopolitical rivalry. The EU and UK have recently increased efforts – also involving other partners – to combat foreign interference.

Foreign information manipulation and interference, and measures to address it

Foreign information manipulation and interference (FIMI), including disinformation, was identified in the [Strategic Compass](#) – a plan of action for the EU's security and defence until 2030 – as a fast-expanding threat to international security and stability, including to the EU and its immediate neighbourhood. The European External Action Service (EEAS) [defines](#) FIMI 'as a pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner ... [by] ... state or non-state actors, including their proxies inside and outside of their own territory.' While foreign interference operations have always been a [part](#) of the geopolitical playbook, new technologies and the internet have changed their scope, nature, and potential reach, making them a risk even for developed democracies. In February 2024, France [uncovered](#) a large Russian disinformation campaign in several EU countries, the UK and the US, aimed at undermining EU support for Ukraine. There is growing potential for exponential growth in the effectiveness and reach of foreign interference, given recent advances in [artificial intelligence \(AI\)](#). The geopolitical landscape has become even more polarised as a result of Russia's aggression against Ukraine, raising the stakes and the threat level to democratic processes. While [China](#) and [Russia](#) are the most well-known countries to engage in foreign interference, they are not the only ones; according to researchers, disinformation is disseminated via social media by over [80 countries](#), and by non-state actors, such as the [Wagner](#) group and linked entities.

The EU has increased its efforts in the past few years to combat FIMI. The East StratCom Task Force (ESTF) was [established](#) in September 2015 as part of the EEAS with the goal of exposing attacks on the EU, its Member States, and its Eastern Neighbourhood, by spreading awareness of pro-Kremlin disinformation, information manipulation, and interference. In its EUvsDisinfo database, the Task Force has compiled, examined, and disproved more than 16 500 [instances](#) of disinformation to date. Later, the EEAS [established](#) two more task forces that deal with the Middle East and North Africa, the Persian Gulf region, and the Western Balkans. A key component of the EU's overall strategy to combat disinformation, the Rapid Alert System (RAS) – one of the four pillars of the [action plan against disinformation](#) – was approved by the European Council in December 2018. It is designed to make it easier for EU institutions and Member States to exchange information about disinformation campaigns and to plan countermeasures. The EEAS has also created a thorough framework and methodology for gathering evidence of FIMI incidents in an organised manner. With the help of an Information Sharing and Analysis Centre (FIMI ISAC), the EEAS is spearheading the initiative to create a '[true defender community](#)'. Furthermore, the EEAS is working closely with the European Commission and Member States to enhance the EU's [FIMI Toolbox](#) – a deliverable of the Strategic Compass, which combines existing tools and new tools to penalise perpetrators. The EEAS also publishes an annual report on FIMI threats. In the second annual report, the EEAS [proposed](#) an evidence- and risk-based framework for responding to FIMI threats (also known as the 'Response Framework to FIMI Threats') that permits the use of adaptive tools linking analysis to action.

Further EU measures include an EU anti-disinformation network in all Member States, which has been [established](#) as part of the European Digital Media Observatory (EDMO), a stand-alone platform that combats disinformation in Europe. On 16 November 2022, the Digital Services Act (DSA) entered into force, and it became directly [applicable](#) across the EU in February 2024 (earlier for large platforms and search engines). It imposes a number of requirements on online intermediary services, such as search engines and social media platforms, to guarantee accountability, transparency, and responsibility for their actions. In February 2024, the Commission [launched](#) a public consultation on DSA guidelines for election integrity. The Code of Practice on Disinformation (CPD), initiated by the EU in 2018 and reinforced in 2022, now has



43 [signatories](#) who have voluntarily made additional commitments, although X has since [withdrawn](#). The DSA [promotes](#) a co-regulatory framework for online harms, comprising codes of conduct, such as the CPD; the [aim](#) of the CPD is to become a code of conduct under the DSA. A [defence of democracy package](#) was proposed by the Commission in December 2023 to combat the threat of foreign meddling in democratic processes more transparently while also promoting civic engagement and citizen participation. It includes a [proposal](#) for a directive on transparency of interest representation on behalf of third countries, and a [recommendation](#) on inclusive and resilient electoral processes in the Union and enhancing the European nature and efficient conduct of the European Parliament elections. The [Hybrid Centre of Excellence](#) – an international, autonomous organisation open to all EU and NATO countries – also plays an important role in, among other things, raising awareness of malign influence. Moreover, the EU is an important [player](#) in international election observation, having sent over 180 election observation missions (EOMs) since 2000. Based on a mandate from MEPs, the EP Secretariat also [works](#) to counter disinformation. It does so for example by producing policy briefs on topics related to disinformation and FIMI, via awareness-raising activities towards e.g. journalists, and through cooperation with institutional and civil society partners.

The UK passed an [online safety bill](#) – [similar](#) to the EU's DSA – in October 2023, which includes provisions to tackle disinformation, harmful content, and other online harms. Online platforms that fail to comply with the regulations outlined in the bill may face significant fines. The UK also established the [National Security Communications Team](#) to address disinformation and protect the public from false information. It works closely with intelligence agencies and other government departments to counter disinformation campaigns. In 2023, the UK [passed](#) legislation introducing a foreign interference offence. In 2022, it launched a [Defending Democracy Taskforce](#) with the stated aim of 'protecting the democratic integrity of the UK', to ensure that electoral processes are secure and resilient, and counter disinformation efforts.

Global cooperation on combating interference in democratic processes

The EU cooperates with many international partners and organisations on combating FIMI, among them NATO, the G7, the US and the UK. EU Member States' [support](#) for the UK following FIMI on Sergey Skripal's poisoning in Salisbury in 2018 – for which Russia denied responsibility – is one example of bilateral cooperation with the UK. More than 20 nations joined Britain in holding Russia accountable for the attack, and expelled more than 120 Russian diplomats in retaliation. Within the G7, leaders [established](#) the G7 Rapid Response Mechanism (G7 RRM) in 2018, the primary goal of which is to combat disinformation propagated by foreign states. The G7 RRM improves cooperation among G7 nations (including the UK, and the EU as a non-enumerated member) in recognising and countering 'diverse and evolving' external challenges to democracy. Disinformation is also a key area of [cooperation](#) between the EU and NATO. For instance, staff-to-staff [exchanges](#) on hostile activities in the information sphere have become common, including with the NATO [StratCom Centre of Excellence](#).

The EU and US [cooperate](#) on FIMI within the framework of the Trade and Technology Council and have, inter alia, adopted a common standard for exchanging structured threat information on FIMI. At their December 2022 summit, the EU and US [agreed](#) to promote their values worldwide through an open, free, global, interoperable, reliable and secure internet, as reflected in the [Declaration for the Future of the Internet](#). It has been signed by more than 70 partners so far, including the EU, its Member States and the UK. Countries also cooperate on disinformation within the United Nations. The UN General Assembly has [welcomed](#) the UN Secretary-General's efforts to foster international cooperation in the fight against disinformation, and the Secretary-General has produced a [report](#) on countering disinformation. In June 2023, the UN unveiled the [Policy Brief on Information Integrity](#), which should lead towards a UN Code of Conduct.

European Parliament position

Parliament set up two consecutive Special Committees on Foreign Interference in all Democratic Processes in the EU, including Disinformation (INGE/ING2), and has [recognised](#) and mapped the threat of foreign interference in all of its manifestations. It offered an assessment of the EU's weaknesses as well as suggestions for bolstering its resilience. Parliament has called for a coordinated strategy to increase the EU's resilience to FIMI, to safeguard the 2024 European Parliament elections, and has [called](#) for increased cooperation and coordination with like-minded partners on combating FIMI. On 8 February 2024, the EP adopted a [resolution](#) inter alia condemning ongoing Russian efforts to undermine European democracy.

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy. © European Union, 2024.