European Parliament

Foreign interference and EU preparedness

Amid escalating geopolitical tensions, deepening political polarisation and widespread adoption of advanced technology, the EU faces the threat of foreign interference. Elections to the European Parliament and in many Member States emphasise the need to defend against foreign interference in a critical time for our democracies.

Foreign interference in the European Union

In the absence of a commonly agreed EU definition, foreign interference is understood to mean any illegitimate interference by foreign powers in the democratic and political processes of the EU and its Member States. Foreign interference covers a wide range of activities, including manipulative online practices, illicit party or campaign financing, covert influence peddling, cybersecurity attacks on electoral infrastructure, and direct action against individuals. A recent Eurobarometer on citizenship and democracy showed that about 8 in 10 Europeans consider that foreign interference in EU democratic systems is a serious problem that should be addressed. Some 74°% agree that such interference can affect citizens' voting behaviour. 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. In January 2024, Russian investigative newspaper *The Insider* reported that Tatjana Ždanoka (Latvia, non-attached after expulsion from the Greens/EFA Group) had been working for the Russian Federal Security Service (FSB). Ždanoka has denied these charges and described herself as 'an agent for peace'. Reportedly, threat actors recently infiltrated spyware tools onto the mobile phones of Members of the Parliament's Subcommittee on Security and Defence (SEDE). Previously, in its 2023 recommendation following investigations into Pegasus and equivalent spyware, Parliament found strong indications that, among others, the governments of Morocco and Rwanda had targeted high-profile EU citizens. These included the President of France, the Minister of the Interior of Spain, the then Prime Minister of Belgium, the former President of the Commission and the former Prime Minister of Italy. Considering these incidents and coinciding with reports from both EU and non-EU countries, it is safe to say that many, if not all, Member States are affected by foreign interference.

EU action to strengthen resilience

Disinformation and manipulation campaigns

The European Commission defined disinformation as 'verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and therefore, may cause public harm'. According to the second EU External Action Service (EEAS) Report on Foreign Information Manipulation and Interference (FIMI) Threats, the EEAS investigated and encoded 750 cases of detected FIMI threats between 1 December 2022 and 30 November 2023. The rise of connectivity, bots and artificial intelligence carries the potential to magnify the volume, velocity and variety of information manipulation and disinformation.

The European University Institute's Media Pluralism Monitor 2022 found that 15 of 32 countries analysed (including the EU's 27 **Member States**) had some form of regulatory framework within which to fight disinformation. However, only the frameworks in Finland, Germany and Lithuania were deemed efficient.

The **EU** has taken both legislative and non-legislative initiatives to combat disinformation. The **Digital Services Act** (DSA) became applicable on 17 February 2024. It aims to prevent illegal and harmful activities online and the spread of disinformation by regulating online intermediaries and platforms. Very large platforms and search engines (VLOPs and VLOSEs) will have to comply with strict obligations and prevent systemic risks, such as the dissemination of misleading or deceptive content (including disinformation), with particular consideration of negative effects on civic discourse and electoral processes. A recent Commission study concludes that the rules hold great potential to reign in Kremlin disinformation campaigns. Not all Member States have officially appointed Digital Services Coordinators, which are, together with the Commission, responsible for the application and enforcement of the DSA. Additionally,

Author: Hendrik Mildebrath, Members' Research Service
PE 760.355 – March 2024

the proposed regulation on the **transparency and targeting of political advertising** (TTPA) should harmonise rules to optimise operation of the internal market regarding sponsored political advertising across Member States and help combat disinformation, information manipulation and interference. The new rules would require public identification of political advertisements and the identity of their sponsor(s), their place of establishment, the amount paid and the origin of the financing. The new regulation would also ban non-EU-based entities from financing political advertisements in the EU three months before an election or referendum organised at EU level or at national, regional or local level in a Member State. The co-legislators are also expected to adopt an **artificial intelligence act** (AI act) that follows a risk-based approach, imposing increasingly strict regulatory burdens the riskier an AI system/practice becomes. It is set to apply, in principle, 24 months after its entry into force. Presumably, AI systems intended for use in influencing the outcome of an election or referendum or the voting behaviour of natural persons would in principle be classified as high-risk and subject to very strict requirements. Where general-purpose AI models negatively affect democratic processes, e.g. by facilitating disinformation, they may pose systemic risks and therefore be subject to heightened obligations. The EU has also taken several non-legislative initiatives, including issuing guidance to strengthen the Code of Practice on Disinformation.

Cyberattacks against electoral infrastructure and individuals

According to the Commission's 2023 recommendation on inclusive and resilient electoral processes in the EU, Member States should, among other things, ensure election-related infrastructure is adequately protected. Member States should take measures ensuring preparedness for, responsiveness to, and recovery from, cybersecurity incidents related to elections, taking into account the requirements established by the **Network and Information Systems 2 Directive** (NIS2), due to be transposed into national law by 18 October 2024. In the same vein, Member States should ensure that more secure hardware and software products are used in elections by taking into account the forthcoming **cyber resilience act**, scheduled for debate during the March plenary. Additionally, the NIS Cooperation Group published a compendium on election cybersecurity and resilience. In its recommendations following the investigation of Europe's **spyware** scandal, Parliament suggested measures that would bolster Member States' use of fundamental rights-compliant spyware, shape a more fundamental-rights compliant spyware market and prevent spyware from falling into the wrong hands. These measures include strengthening EU export controls, partnering with like-minded countries and ostracising malign spyware vendors, and adopting rigorous controls for intelligence development policies.

Lobbying on behalf of third countries

Only 15 Member States regulate the transparency of interest-representation activities and have a register on interest-representation activities. These regulatory frameworks are highly fragmented. As part of its defence of democracy package, the Commission tabled a proposal regarding the transparency of foreign interest representation on 12 December 2023.

Other policy interventions include updating rules governing European political parties and foundations, supporting free and plural media, addressing questions of third-country investment in electoral infrastructure, and anti-money laundering and corruption. The EU has also sanctioned Russian-origin media outlets. An in-depth analysis requested by the Special Committee on foreign interference in all democratic processes in the European Union, including disinformation (ING2), suggests criminalising foreign interference and banning foreign and foreign-funded third-party election campaigning.

European Parliament role

Besides negotiating and enacting the above-mentioned laws as co-legislator, Parliament has also taken non-legislative action, including launching the INGE and ING2 Special Committees and the PEGA Committee of Inquiry. Parliament has also adopted resolutions on topical issues, such as on suspicions of corruption linked to Qatar and on allegations of Russian interference.