Foreign interference in all democratic processes in the European Union, including disinformation

2020/2268(INI) - 09/03/2022 - Text adopted by Parliament, single reading

The European Parliament adopted by 552 votes to 81, with 60 abstentions, a resolution on foreign interference in all EU democratic processes, including disinformation.

Need for a coordinated EU strategy against foreign interference

Members are concerned about the growing incidence and increasingly sophisticated nature of attempts at foreign interference and manipulation of information, mainly by Russia and China, targeting all aspects of the democratic functioning of the European Union and its Member States.

The resolution noted that Russia engaged in disinformation on an unparallel malice and magnitude in the run-up to and during the war of aggression against Ukraine, proving that even information can be weaponised.

Parliament welcomed the recent EU-wide ban on Russian propaganda channels such as Sputnik TV, RT (formerly Russia Today) and other Russian disinformation outlets.

Members are concerned about the many **gaps and loopholes** in current legislation and policies at EU and national level aimed at detecting, preventing and combating foreign interference. They are concerned about the **lack of awareness of the seriousness of the current threats** posed by foreign authoritarian regimes and other malicious actors, as well as the lack of appropriate and sufficient standards and measures to identify and respond to acts of foreign interference.

The Commission is called on to propose a **multi-layer, coordinated and cross-sector strategy**, as well as adequate financial resources, aimed at equipping the EU and its Member States with appropriate foresight and resilience policies and deterrence tools.

This strategy should be built on:

(a) **common terminologies and definitions**, a single methodology, evaluations and ex post impact assessments of the legislation adopted so far, a shared intelligence system, and understanding, monitoring, including early warnings, and situational awareness of the issues at stake;

(b) **concrete policies** enabling resilience-building among EU citizens in line with democratic values, including through support to civil society;

(c) **appropriate disruption and defence capabilities**;

(d) **diplomatic and deterrence responses**, including an EU toolbox for countering foreign interference and influence operations, including hybrid operations, through adequate measures, e.g. attribution and naming of perpetrators, sanctions and countermeasures, and global partnerships to exchange practices and promote international norms of responsible state behaviour.

In particular, Members called on the EU and its Member States to increase the resources and means allocated to bodies and associations in Europe and around the world, such as think tanks and fact-checkers, responsible for monitoring threats, including disinformation, and raising awareness of their severity.

Strategy sectors

The strategy should be based on a risk-based, whole-of-society and whole-of-government approach, covering the following areas in particular:

- building resilience through situational awareness, media and information literacy, media pluralism, independent journalism and education: EU public funding should be allocated to independent fact-checkers, researchers, quality investigative media and competent investigative journalists, as well as to NGOs that research and investigate information manipulation and interference;

- foreign interference using online platforms: Members called for regulation and actions to oblige platforms, especially those that pose a systemic risk to society, to do their part to reduce information manipulation and interference, and to cooperate with the competent authorities to test their systems regularly;

- strengthening critical infrastructure and strategic sectors: Members recommended implementing a common strategy to respond to cyber-attacks on critical infrastructure, extending the list of critical entities to education systems and digital electoral infrastructure, and establishing a secure, sustainable and equitable supply of raw materials used to produce critical components and technologies, including batteries;

- combating foreign interference during electoral processes: the protection of the entire electoral process should be made a top EU and national security issue. The Commission is invited to develop a better response framework to counter foreign interference in electoral processes;

- covert funding of political activities from foreign actors and donors: participation in any covert activity funded by foreign actors which aims to influence the European or national policy process should be made illegal in all Member States;

- cyber security and resilience to cyber attacks: investment should be increased in the EU's strategic digital capacities and skills to detect and combat foreign interference, such as artificial intelligence, secure communication and data and cloud infrastructures. Members condemned the widespread use by foreign actors of illegal and large-scale surveillance programmes, such as Pegasus, to target journalists, human rights activists, academics and politicians, including European heads of state;

- interference by foreign actors through recruitment of high-level personalities, national diasporas, universities and cultural events: Members condemned all types of elite capture and the technique of co-opting high-level officials and former EU politicians used by foreign companies with links to governments that interfere against the EU. They are concerned about cases of covert funding of research in Europe, as well as Chinese attempts to poach talent through Confucius Institute scholarships;

- deterrence, accountability and collective counter-measures, including sanctions: Members called for further action against foreign interference, especially when it takes the form of large-scale disinformation campaigns, hybrid threats and hybrid wars, including the establishment of a sanctions regime;

- multilateral global cooperation in relevant international fora between like-minded countries in the form of a partnership based on common understanding and shared definitions, with a view to establishing international norms and principles.

The Commission is called on to consider, together with the EEAS, the establishment of an independent and well-resourced **European Centre for Interference Treats** and Information Integrity to identify, analyse and document information manipulation operations and threats of interference against the Union as a whole.