Taking stock of the follow-up taken by the EEAS two years after the EP Report on EU strategic communication to counteract propaganda against it by third parties. Recommendation to the Vice President/High Representative of the Union for Foreign Affairs and Security Policy and to the Council

2018/2115(INI) - 13/03/2019 - Text adopted by Parliament, single reading

The European Parliament adopted by 489 votes to 148 with 30 abstentions a resolution containing a recommendation to the Council and the Vice President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy concerning taking stock of the follow-up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda against it by third parties.

State of play 2018 - Tackling hybrid warfare

Parliament underlined that freedom of speech and expression as well as media pluralism are at the heart of resilient democratic societies, and provide the best safeguards against disinformation campaigns and hostile propaganda. It proposed to the European Council that counteracting disinformation and hostile propaganda should be given priority with sufficient resources and instruments to safeguard objective reporting and dissemination of information.

It suggested developing a legal framework both at EU and international level for tackling hybrid threats, including cyber and information warfare, that would allow for a robust response by the Union, covering targeted sanctions against those responsible for orchestrating these campaigns.

The VP/HR and the Commission were called on to become more closely involved in this area by preparing a thorough assessment of the new regulations, including the General Data Protection Regulation (GDPR) and the upcoming e-Privacy Regulation, as a safeguard against malicious use of social platforms.

Member States were called on to:

- invest proactively in educational measures that explain the different ways of producing and disseminating disinformation in order to improve citizens’ ability to detect and respond to disinformation;

- ensure an effective exchange of information between all of their relevant authorities for tackling propaganda, manipulation and disinformation, including the cyber and information warfare.

Misinformation, disinformation and propaganda targeting the EU and its neighbours

Members recommend adapting the EU's and Member States' response to the continuously growing sophistication of the tools used to create and to spread disinformation, including the new ways of spreading propaganda by using multiple low-level websites, private messaging apps, search engine optimisation, online news portals and TV stations to disseminate the main narratives.

They strongly condemned the increasingly aggressive actions of Russia, China, Iran, North Korea and others in this context, which seek to undermine or suspend the normative foundations and principles of European democracies and the sovereignty of all Eastern Partnership countries, as well as influence elections and support extremist movements, taking into account that the scale of cyber attacks is constantly growing.

Industry and social media

While acknowledging a new investment of effort by social media companies to tackle disinformation, Members stressed that special attention should be paid to the effective implementation of the EU Code of Practice on Disinformation. They recommended regulating the actions of social media companies, messenger services and search engine providers and making it possible to uncover the identity and location not only of the authors, but also of the sponsors of the submitted political content. Parliament wanted to ensure that companies are held to account for the social impact of automated recommendation systems that promote disinformation, stressing that companies have a responsibility to speedily take down systemic fake news. Technology companies were called upon to invest more in tools identifying propaganda, in improving online accountability and in ensuring better identity checks of users before joining the respective platforms in order to eliminate botnets, as well in reducing financial incentives for those who profit from disinformation. Social media companies must react urgently when suspicious content of a political nature is disseminated, particularly if it incites to hate or crime.

Safeguarding elections from hostile propaganda

Members strongly condemned the interference of third parties of any kind, including private companies, in elections and referenda, and the malicious use of bots, algorithms, artificial intelligence, trolls, deep fakes and fake accounts in political campaigns and called on the Member States affected to urgently conduct, with the support of Eurojust if necessary, thorough investigations into these hostile campaigns.

They were concerned about recent developments in the algorithms of large social networks and their potentially harmful role in highlighting content containing false information or hate speech. They invited Member States to ensure that electoral laws take into account possible threats stemming from disinformation campaigns, cyber attacks, cybercrimes and violations of freedom of expression when voting. These laws should be adequately amended to enable Member States to effectively and proactively counteract such threats. Member States were asked to adapt their electoral rules on online campaigning, and to monitor the transparency features in relation to political advertising introduced by the online platforms.

Parliament called for legislation to address data use in election campaigning, following the exposure of data misuse by Cambridge Analytica in the 2016 UK referendum campaign, in order to further safeguard future election campaigns from undue influence.

Best practices

Parliament stressed the need to develop greater resilience based on all-government and all-society approaches, and the ability to respond to threats in real time, develop pre-emptive and proactive measures and think one step ahead, rather than merely reacting to and analysing attacks that have already taken place in the cyber and information domains. It recommended drawing attention to the technical progress in this field and sharing examples of best practice in the form of measures already taken by individual Member States, while developing ways of fostering close cooperation with the United Kingdom after Brexit, and working in cooperation with the intelligence community and allies such as the US and Canada, NATO and the EU Intelligence and Situation Centre.