Council of the
European Union

Brussels, 19 June 2019
(OR. en)

10415/19

INST 171
AG 25
PE 230
DATAPROTECT 171
JAI 727
CYBER 209
FREMP 86
RELEX 624
JAIEX 101
HYBRID 27
CULT 95
EDUC 327
AUDIO 90
DIGIT 116
INF 193

COVER NOTE

From:	Presidency of the Council of the European Union
To:	Delegations
Subject:	Report of the Presidency to the European Council on 20-21 June 2019, on countering disinformation and the lessons learnt from the European elections

Delegations will find attached the report of the Presidency to the European Council on countering disinformation and the lessons learnt from the European elections.

Report of the Presidency to the European Council on 20-21 June 2019, on countering disinformation and the lessons learnt from the European elections

In March 2019 the European Council called for further enhanced coordinated efforts to address the internal and external aspects of disinformation and protect European and national elections across the EU. It also tasked the Presidency, in cooperation with the European Commission and the High Representative, to present a report based on the lessons learnt, in order to inform the EU's long-term response.

Based on this, the Presidency has continued its work to secure free and fair elections and to ensure a coordinated response at Council level to the challenges posed by disinformation. The Presidency finalised the report[1] on the mapping exercise on existing structures and measures taken by the Member States to counter disinformation, organised a policy debate in the Education, Youth, Culture and Sport Council (May 2019) on tackling disinformation in order to rebuild EU citizens' trust in the media, organised events relating to the resilience of societies within the EU[2] and in its neighbourhood[3], and has regularly followed the implementation of the Action Plan against Disinformation[4] and the elections package[5] in the Council Working Group.

I. Overview of disinformation narratives and threats in the context of the elections

An overall preliminary evaluation points to the fact that disinformation campaigns have used narratives that aim to undermine **trust in democracy** and in the EU, its policies and core values by aiming to polarise European societies, exploit divisive public debates and create a climate of mistrust. It aims to create internal tensions in the Member States, attack the pillars of democracy and influence the involvement of citizens in the democratic process, including attempts to influence voters' preferences and suppress the vote.

[1] 10015/19.
[2] Conference on 'Greater resilience to ensure free and fair elections', 1 April 2019, Brussels.
[3] Launch of the study 'Dimensions of Risk and Resilience in the Western Balkans: regional vulnerabilities to malign influence', developed by Global Focus, 22 May 2019, Brussels.
[4] 15431/18.
[5] 12130/18, 12321/1/18REV; 12404/18; 12405/18.

There are multiple **methods of interference in the democratic process**: information manipulation (disinformation, non-transparent political advertisement, sentiment amplification, fake online identities); cyber-attacks (attacks on infrastructure, hacking, 'hack and leak' operations); co-opting of elites; and the financing of political parties or private entities. The difficulty of identifying the sources, attributing disinformation campaigns, together with their changing nature and increasing sophistication require continuous assessment and an appropriate response.

Measures at EU and Member State levels in close cooperation with the media, civil society and various networks of fact checkers clearly raised public awareness in the run-up to elections.

II. Preparedness measures in the context of the European elections

II.1. Main activities at Council level

A. Mapping the Member States' capacities and measures to counter disinformation

Based on the Action Plan against Disinformation and the Council conclusions adopted in February on securing free and fair elections, the Presidency launched a mapping exercise through a questionnaire, designed to identify capacities and measures in all Member States to counter disinformation, in the context of the European Parliament elections and beyond. The answers provided an outline of the situation in the Member States and facilitated the identification of ways forward.

Through the mapping exercise, the Presidency has gathered relevant information and identified some common trends, approaches and challenges, such as:

- The **approach to tackling disinformation** varies greatly across Member States. Responsibilities in the field are usually shared across a large number of ministries, with coordination carried out by the Prime Minister's office or one lead ministry. The same trend is found at EU level, where EU institutions are actively involved in the fight against disinformation (in particular, various Directorate-Generals of the Commission and the EEAS' East Strategic Communication Task Force and Hybrid Fusion Cell).

- **Ways of combating disinformation** differ among Member States and depend on the human resources deployed and the technology used. Some Member States have specialised posts in the field and have invested in technology and developed strategies to tackle disinformation, while in others, the issue is addressed mainly by journalists and

academics, who might then work in conjunction with technology companies to raise awareness of the importance of (media) literacy.

- **Definitions of 'disinformation'** used at national level are, in general, kept broad. The main difficulty lies in assessing whether information is false and has been spread with the intention of deceiving the public and causing public harm, and whether acting on it could be considered harmful to freedom of expression. Only a small number of Member States have a specific **legislative framework** in place to sanction the dissemination of disinformation by state or non-state actors.

- On average, the **perception of the threat level** in society is assessed as being medium to low. Online platforms have become important gateways to information and, as such, play a distinct role as a vehicle with the potential to spread possibly harmful information. Further assessment of the responsibility of online platforms was requested by several Member States. In this regard, in the period between January and May 2019, the commitments undertaken by online platforms in the self-regulatory Code of Practice on Disinformation were monitored particularly closely by the Commission. By the end of 2019, the Commission will carry out an assessment of the effectiveness of the Code of Practice and propose further initiatives, including of a regulatory nature, if necessary. In terms of the **impact of disinformation campaigns on different groups**, respondents identified young people, senior citizens and persons belonging to different types of minorities as being among the most vulnerable.

- The main **topics of disinformation campaigns** concern the exploitation of 'wedge issues' such as migration, terrorism, the EU and the role of the Member States within the EU, the Euro-Atlantic architecture, climate change, religious and ethnic tensions, or health issues. Member States distinguish between different types of disinformation campaigns: those based on purely fabricated news and those based on half-truths, which are more difficult to refute.

- The most **common challenges** are: striking the right balance between freedom of speech and countering disinformation; the lack of coordination at national level; insufficient media literacy and critical thinking among the general public; a lack of understanding of the nature of the problem; and the exposure of certain vulnerable groups.

B. Work in the Education, Culture, Youth and Sports Council

On 23 May 2019, the Council held a policy debate entitled "From tackling disinformation to rebuilding EU citizens' trust in the media", based on a Presidency discussion paper[6]. The ministers of culture and audiovisual media stressed that quality journalism, media freedom and pluralism remain the cornerstones of today's European audiovisual landscape (also ensured by the new Copyright Directive and the Creative Europe programme). Media literacy skills are considered to be of utmost importance in order to enable European citizens to make informed decisions and to develop their critical thinking in relation to the media content they consume, create and promote, thus raising awareness of disinformation (the revised *Audiovisual Media Services Directive* creates, for the first time, an obligation for Member States to promote and develop media literacy skills). The establishment of a European network of fact checkers is considered essential for consolidated action at EU level, while new measures to complement the self-regulatory and co-regulatory initiatives currently in place need to be considered. Transparency in the activities carried out by the platforms and the algorithms they use, the establishment of clear rules for online political advertising, and the removal of fake accounts were mentioned as important elements in the fight against disinformation.

C. Restrictive measures against cyber-attacks threatening the Union or its Member States

In May 2019, the Council adopted a Decision and a Regulation[7] establishing a framework enabling the EU to impose sanctions or other restrictive measures (e.g. asset freeze, travel ban) against cyber-attacks which constitute an external threat to the Union or its Member States, including cyber-attacks against third States or international organisations where restrictive measures are considered necessary to achieve the objectives of the Common Foreign and Security Policy.

D. Infringements of relevant data protection rules including appropriate sanctions, data processing and analysis for political purposes

As part of the electoral package, the Council and the Parliament amended the Regulation on the European political parties and foundations at European level, which entered into force in March 2019. The new rules introduced sanctions for the European political parties that abuse data protection rules to attempt to influence the outcome of European elections.

---

[6] ST 8808/19 INIT.

[7] Council Decision (CFSP) 2019/797 and Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

The Commission also recommended that Member States apply appropriate sanctions on political parties and foundations at national and regional level for infringements of rules on the protection of personal data with the aim of deliberately influencing elections.

II.2 Activities of other institutions

E. Update on the activities of the election cooperation networks

In September 2018, the Commission adopted a package of measures to support the securing of free and fair elections in Europe. An important step in the implementation of the package was the establishment of national networks of responsible authorities to cooperate in preparations for elections, and their coordination at European level. The national networks facilitated the rapid and secure exchange of information on issues capable of affecting the elections: the identification of threats and gaps, the sharing of findings and expertise, and liaison on the enforcement of relevant rules in the online environment.

The European cooperation network for elections, which brings together the contact points of the national elections networks, met four times in 2019: on 21 January, 27 February, 4 April and 7 June. The meetings focused on concrete and practical exchanges on a range of topics[8] relevant to protecting European elections and building more resilient electoral systems.

The meeting on 7 June took stock of the conduct of elections, the threats identified and the solutions found and implemented. It allowed for a first reflection on the outcome of the Member States' and EU institutions' efforts in this area. It was agreed with the Member States that the network would continue its work in the following years, with bi-annual meetings.

F. Rapid Alert System: update on its roll-out, level of activities and relevant alerts, particularly in the context of European elections

The newly established Rapid Alert System became operational on 18 March 2019 and makes it easier for Member States and EU institutions to share media monitoring and trends reports, and insights and best practices on how to address disinformation campaigns.

[8] These included: data protection in the electoral context, structure and operation of national elections networks, ensuring transparency of political advertising and campaign financing, engagement with social media platforms and ensuring equality of treatment in access to support and data, conventional electoral safeguards in the online context, cybersecurity, the role of media regulators, and awareness-raising initiatives.

The three meetings of the national contact points focused on the functionality, workflow and working methods of the Rapid Alert System, cooperation with online platforms and international partners, and lessons learnt from the monitoring of the disinformation campaigns which affected the European elections. The members participated in the exercise conducted by the European Centre of Excellence for Countering Hybrid Threats, which focused on the ability to recognise hostile information operations, upgrade capacities for contingency planning and evaluate different response strategies to hybrid threats.

There is a strong interplay between the Rapid Alert System and the elections networks. In the Rapid Alert System meeting in Tallinn on 3 and 4 June, after the EP elections, one of the main conclusions was that the Rapid Alert System was a useful tool to increase situational awareness and share understanding of the issue. It is important to realise that, while elections may recede into the background in the short term, the basic structures must be prepared and strengthened.

G. Efforts to enhance transparency in political advertising and relations with platforms

In the elections package, the Commission called on Member States, national political parties, foundations and campaign organisations to encourage and facilitate the transparency of paid online political advertisements and communications, encourage the disclosure of information on campaign expenditure for online activities and the disclosure of information on any targeting criteria used in the dissemination of such advertisements and communications.

On 15 March 2019, Commissioner Jourová called on national political parties and foundations, in line with the Commission Recommendation, to ensure the transparency of political advertising, implement specific and appropriate measures to prevent cyber incidents, and respect European data protection rules during the campaign. Furthermore, a meeting was held with Secretaries-General of the European political parties and foundations to present the Commission's initiatives in the context of free and fair elections.

H. Code of Practice on Disinformation: implementation and assessment of industry's adherence to it during the European elections

On the basis of reports submitted each month from January to May 2019, the Commission, in cooperation with the European Regulators Group for Audiovisual Media Services, monitored actions taken by Facebook, Google and Twitter to ensure the integrity of the elections.

All three platforms implemented political ad transparency, including the labelling of political ads and the creation of publicly accessible political ads libraries that are searchable through appropriate interfaces. However, only Facebook extended transparency measures to issue-based advertising. In addition, all three platforms took substantial action to ensure the integrity of their services and protect them from manipulative behaviour, including coordinated disinformation operations and the malicious use of bots and fake accounts. The platforms also provided data on measures taken to improve the scrutiny of ad placements and reduce the advertising revenues of purveyors of disinformation. However, more needs to be done. Platforms should, for instance, provide researchers with the necessary data, in line with personal data protection rules. Cooperation with researchers will enable a better understanding of disinformation campaigns and enhanced monitoring of the Code of Practice implementation.

I. Cybersecurity and the resilience of election infrastructure

To address the growing risks of cyber incidents, the elections package included a recommendation urging Member States to adopt security measures to mitigate risks as outlined in the compendium on the cybersecurity of election technology issued by the Network and Information Systems Cooperation Group.

On 5 April 2019, the Commission, the European Parliament and the European Union Agency for Network and Information Security (ENISA) co-organised a cyber preparedness exercise with Member State authorities, which tested the preparedness of election mechanisms to tackle cyber crises, ensure cooperation and strengthen situational awareness. More than 80 representatives participated in this first EU table-top exercise.

In addition, in May 2019, ENISA organised an additional exercise simulating cyber-attacks on critical infrastructures before and during European elections.

J. Other measures including awareness-raising campaigns

With a view to enhancing the role of fact checkers and research organisations, a new project under Horizon 2020 was launched in November 2018 to create the Social Observatory for Disinformation and Social Media Analysis (SOMA), which 14 European fact-checking organisations have already joined. To foster media literacy in Europe, the Commission organised a first European Media Literacy Week from 18 to 22 March 2019, featuring more than 320 events throughout Europe. The EU institutions jointly conducted numerous awareness-raising activities and public events across the EU Member States on the negative impact of disinformation, specifically targeting multipliers (more than 300 journalists were reached), and distributed information and audiovisual media material to the

public on attempts by Russian sources to interfere in electoral processes, as well as the counter-measures prepared by European External Action Service's East Strategic Communication Task Force.

III. Conclusions and input for future actions

The preliminary evaluation of the disruptive role of disinformation in the context and in the wake of the latest European elections reflects the continuous evolution of disinformation and its capacity to adapt to changing technology.

This underlines the need for a **permanent state of preparedness and a permanent process to tackle the problem,** combining bottom-up and top-down approaches, and through pre-emptive engagement and close cooperation with the relevant stakeholders such as academia, media, civil society, fact checkers and social platforms.

The central focus of all measures and commitments should be citizens' rights and interests. Efforts to combat disinformation, in particular in the context of elections and the democratic debate, must comply with the Union's shared values of respect for democracy, rule of law and fundamental rights. The right to freedom of association at all levels, such as in political and civic matters, and the right to freedom of expression, which includes the freedom to hold opinions and to receive and impart information and ideas without interference from public authorities and regardless of frontiers, are fundamental rights of every citizen of the Union.

The bottom-up approach enhances critical thinking and societal resilience through media/digital/digital-civic literacy, in order to increase understanding and trust in democratic process and policies.

The top-down approach includes increased and permanent coordination between the EU Member States - at all governance levels and in all relevant fields (education, media, cybersecurity, etc.) - in order to reduce inequalities among citizens (as vulnerable categories are more exposed to disinformation), deliver sustainable institutional infrastructure and norms as well as enhance threat awareness and engagement with citizens.

In this vein, the strategic **European and national approaches towards disinformation** should focus on at least three main strands of actions:

1. **Calibrated responses** to malign interference and disinformation – meaning that improved and tailored instruments should be used against disinformation campaigns while ensuring the preservation of fundamental democratic values.

2. A coordinated response involving **proactive and reactive approaches to ensure** long-term and sustainable results. A strong and healthy democratic society should continuously strive to maintain an adequate level of threat awareness among the public and media, raise societal resilience to information attacks by promoting media literacy/critical thinking, provide citizens with the necessary tools to better detect disinformation, and support high-quality independent media. The capacity to ensure preparedness should benefit from adequate financial, human, technological and institutional resources.

3. The approach should also aim to produce a better understanding of the **levels of awareness** of disinformation among the different categories of the population and to tailor the responses on this basis. The role of fact checkers and multidisciplinary academic researchers is paramount in this regard. Against this background, and in order to broaden cooperation between them and to promote a deeper understanding of the phenomenon of online disinformation, the Commission is expected to launch a secure European online platform under the Connecting Europe Facility in the second half of 2019.

Reflection is also needed on the **existing legal and institutional framework** – both at national and European level. The Commission's monitoring of the measures taken by the various platforms in the months prior to the European Parliament elections indicates that there is **more work to be done in terms of increasing transparency**, improving access to data in order to facilitate research, and identifying and rapidly blocking fake accounts and bots. Independent fact checkers and researchers also play an important role in monitoring the effectiveness of the Code of Practice as well as in furthering understanding of the structures that sustain disinformation and its dissemination online. The opportunity should be taken, led by the Commission, to conduct an in-depth evaluation of the implementation of commitments undertaken by online platforms and other signatories under the Code of Practice, and discuss further commitments and follow-up actions with the platforms at EU level.

Furthermore, there are good grounds to consider **consolidating structures at EU level,** such as by establishing a permanent horizontal working party of the Council of the EU, which would have a coordinating role and would monitor possible threats to democratic processes in order to enhance resilience and counter hybrid threats. In this context, the Romanian Presidency, together with the upcoming Finnish and Croatian presidencies (as

the Trio Presidency of the Council of the European Union) has presented the Member States with a clear proposal for a mandate for this horizontal working party. The purpose is to foster the coherence and coordination of the work at Council level on enhancing resilience and countering hybrid threats.

Existing cooperation structures such as the European elections networks and the Rapid Alert System make an important contribution to common situational awareness and the sharing of analysis. These structures must be maintained and potential improvements discussed.

In the context of the Rapid Alert System, the work done so far has been crucial in building a community of practitioners who will be able to develop common methods to better detect, analyse and expose disinformation in the long term. The future activities of the Rapid Alert System and the strengthening of its cooperation with online platforms and with international partners such as the G7 and NATO will further contribute to the efforts to protect European democracies from disinformation. This work has also built on the experience and ongoing work of the East Strategic Communication Task Force and their considerably increased capabilities in detecting, analysing and exposing disinformation from Russian sources[9]. All these should be complemented with relevant and up-to-date risk and threat assessment and analysis, performed both at national and EU level. Adequate financial means and improved technological capabilities to adjust to ever-changing threats will be required in order to continuously tackle the problem.

The mapping exercise initiated by the Romanian Presidency has provided a clearer image of the state of play regarding the efforts undertaken at national level in order to combat disinformation. The progress made and the lessons learnt in the recent context of European and national elections and by closely monitoring the evolution of technology and disinformation (as the trend suggests that they go hand in hand) could be followed up with regular progress reports from the Commission and the High Representative to the Council on the long-term response to disinformation, and **a repeat of the mapping exercise** in the next two or three years, together with an assessment of the effectiveness of the Action Plan against Disinformation.

[9] As regards the work of the East Strategic Communication Task Force, from January onwards, comprehensive monitoring, data analysis and exposure of disinformation spread by Russian sources is now conducted in six EU languages, Russian, and the languages of Eastern Partnership countries, presented on the EUvsDisinfo.eu portal and shared through the Rapid Alert System. The number of disinformation cases linked to Russian sources and documented by the East Strategic Communication Task Force since January 2019 (998) has more than doubled in comparison with the same period in 2018 (434)