COMBATING DISINFORMATION

cep**PolicyBrief** No. 2019-14

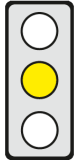Centrum für
Europäische Politik

KEY ISSUES

Objective of the Communication: The EU and Member States will be enabled to combat disinformation more effectively, particularly on the internet.

Affected parties: Advertisers, online platforms, fact-checkers, whole population

Pro: (1) The development of a network between national authorities facilitates the sharing of intelligence which facilitates efforts to combat disinformation.

(2) By relying on a voluntary obligation, the Code of Practice for online platform operators balances the interests of the Commission and the technical and economic possibilities of platform operators.

Contra: The Commission's threat to turn the Code of Practice into law violates the freedom of the media.

The most important passages in the text are indicated by a line in the margin.

CONTENT

Title

Joint Communication from the High Representative of the Union for Foreign Affairs and Security Policy and the European Commission **JOIN(2018) 36** of 5 December 2018: **Action Plan against Disinformation**

Brief Summary

▶ **Context and objectives**
  – The free exchange of opinions, information and ideas is essential in a democracy (p. 1).
    - It enables citizens to form and express their opinions which is necessary for participation in political processes - e.g. elections and demonstrations.
    - It is protected as a fundamental right in the Member States and under Art. 11 Charter of Fundamental Rights of the EU (CFR).
  – The systematic distribution of false information (hereinafter "disinformation") threatens the freedom of citizens to form an opinion and is thus also a threat to fair democratic processes.
  – To be specific, disinformation (p. 1)
    - does not involve statements that are banned per se (in Germany it is illegal to deny the holocaust),
    - but does involve verifiably false or misleading information and/or narratives on a variety of subjects - e.g. health, crime, foreign policy, contemporary history -,
    - is created by state and/or non-state actors for economic gain or in order to deceive the public and
    - may harm the public interest, such as protection of health, security and the environment.
  – The spread of disinformation is increasingly occurring via social media - e.g. Twitter, Facebook (p. 2, 4).
    - Those wishing to spread disinformation often make extensive use of false user accounts (fake accounts) some of which are controlled by computer programmes (bots) in order to
      - manipulate user ratings, opinions or trends on social media and/or
      - disseminate manipulated videos or images which use computer technology to depict events which never actually occurred but look deceptively realistic - e.g. alleged interview statements by politicians.
  – For the EU, its Member States and partner countries - e.g. the Ukraine - disinformation campaigns from outside the EU also form part of "hybrid threats" (p. 3-4). "Hybrid threats"
    - are aimed at influencing public opinion and/or destabilising society in another country while remaining below the threshold of formally declared warfare and
    - are characterised by the simultaneous use of various conventional and unconventional methods - e.g. economic sanctions, computer attacks, disinformation campaigns.
  – Against this backdrop, the European Council called on the Commission and the European External Action Service (EEAS) to devise an Action Plan to combat disinformation. The plan is based on four pillars.

▶ **Pillar 1: Expand the EEAS**
  – The following EU units will be expanded to combat disinformation from and in third countries (p. 5-6):
    - the EU delegations under the EEAS that represent the EU as "embassies" in third countries,
    - the central "EU Hybrid Fusion Cell" of the EEAS which is responsible for analysing and sharing classified and open source information of Member States [JOIN (2016) 18, p. 4],

Authors: Dr. Matthias Kullas and Muhammed Elemenler, LL.M. | kullas@cep.eu

- the "East StratCom" Task Force [Ref. Ares (2015) 2608242, p. 3] (p. 4), within the "Strategic Communications Department" of the EEAS, which in the eastern European EU partner countries of Armenia, Azerbaijan, Georgia, Moldova, Ukraine and Belarus,
  - debunks disinformation,
  - supports the independence of the media environment and
  - targets information about the EU and EU policy at the church, political parties and other social players.
- In order to expand capacity, EU funds for these three units will be increased from € 1.9 million to € 5 million. Specifically, this is to finance (p. 5-6)
  - the employment of 50 additional specialist staff - e.g. data analysis experts - and
  - the acquisition of analysis tools - e.g. software, contracts with media monitoring services.
– The other two task forces within the "Strategic Communications Department", "Western Balkans Task Force" - for Albania, Bosnia-Herzegovina, Kosovo, Montenegro, North Macedonia and Serbia - and "Task Force South" - for countries in the Middle East, North Africa and the Gulf region - will receive a mandate to combat disinformation.

► **Pillar 2: Digital coordination and "Rapid Alert System" between Member States**
  – The agencies in the Member States handling disinformation will be coordinated in a digital network. This digital network will
  - have a "Rapid Alert System" enabling alerts about disinformation campaigns to be shared between national agencies in real-time (p. 7),
  - facilitate the sharing of intelligence and methods between Member States and the EU such as regarding
    - trends, disinformation strategies and research projects (p. 8) and
    - possibilities for raising awareness of disinformation and effective communication strategies (p. 8).
  – EU institutions and the Member States will (p. 8)
  - coordinate their public relations work to combat disinformation and
  - pro-actively communicate the values and policies of the EU (such as by way of national websites on myths about the EU).

► **Pillar 3: Code of Practice for advertisers and online platforms**
  – The spread of disinformation is to be contained. The Commission has agreed a non-binding Code of Practice with advertisers – e.g. advertising agencies – and online platforms (especially social media platforms) [COM(2018) 236, S. 7-9]. This Code of Practice provides inter alia that
  - advertisers should limit the placement of adverts on internet sites that spread disinformation thereby reducing the revenues of the purveyors of disinformation and
  - online platforms
    - must use technologies that prioritise relevant, authentic and credible information,
    - must close fake accounts,
    - must separate sponsored content – e.g. political and subject-related advertising – from editorial content and identify it as such, and
    - must identify "bots" as such so that internet users can distinguish them from human beings.
  – The Commission will (p. 9)
  - monitor the implementation of the Code of Practice and report on it and
  - after one year assess the Code of Practice together with national media supervisory authorities.
  – If the "efforts" of online platforms to implement the Code of Practice are inadequate, the Commission will take regulatory action.

► **Pillar 4: Greater public understanding and awareness of disinformation**
  – Understanding of disinformation and its effects will be improved. For this purpose, the Commission will (p. 10)
  - support the development of an independent European network of fact-checkers and academic researchers by co-financing its technical equipment and infrastructure (Social Observatory for Disinformation and Social Media Analysis, SOMA), and
  - support research and the fight against disinformation inter alia by the European Research Framework Programme "Horizon Europe".
  – Public awareness of disinformation will be raised. For this purpose, the Commission will (p. 11)
  - work with the EEAS to increase communication with the public on disinformation in neighbouring countries,
  - promote the media literacy of its own population by
    - calling on Member States, inter alia together with media service providers such as YouTube, to increase media literacy in all areas of society and for all ages [see Art. 33a Directive on audio-visual media services (EU) 2018/1808],
    - facilitating the collaboration of media literacy experts (in a Medialiteracyweek),

Policy Context

As early as 2015, as a result of Russian disinformation campaigns in eastern EU partner countries, the European Council requested the High Representative of the Union for Foreign Affairs and Security Policy for concrete action [Conclusions of 19 and 20 March 2015, EUCO 11/15], which resulted in the establishment of the "East StratCom Task Force". Against the backdrop of disinformation campaigns during the US presidential election in 2016, the Commission turned its attention to proposals for combating disinformation [cf. Communication COM(2018) 236]. In 2018, the European Council called on the Commission and the High Representative to develop an Action Plan [Conclusions of 28 June 2018, EUCO 9/18].

Options for Influencing the Political Process

European Institution: EEAS (leading)
Committees of the European Parliament: Internal Market and Consumer Protection
Federal Ministries: Foreign Affairs (leading)
Committees of the German Bundestag: Foreign Affairs (leading), Internal Affairs, EU, Economic Affairs, Legal Affairs

ASSESSMENT

Economic Impact Assessment

Disinformation can lead to inappropriate political decisions and fuel developments which threaten social cohesion. Disinformation is not a new phenomenon. New is the fact that disinformation is increasingly being spread on social media. Social media is particularly suitable for this as disinformation can be spread at high speed, with a vast reach and without any checks on the content. This is a particularly effective way to send falsified images or images taken out of context that cause an angry reaction in those viewing them. In addition, social media enables disinformation to be accurately targeted so that people receive individualised disinformation which can further increase its effectiveness. Disinformation was very successfully disseminated on social media during the US presidential elections for example. Attempts were also made to influence the French presidential elections and the Brexit referendum using disinformation campaigns on social media. Against this backdrop, it is appropriate that the High Representative for Foreign Affairs and Security Policy and the European Commission are submitting an action plan to combat disinformation.

The chosen definition of disinformation reflects a key problem: disinformation cannot solely be defined according to whether the information - which is damaging to the public interest - is true or false because, firstly, not all false information - e.g. transposed digits - constitutes disinformation. Secondly, the cross-over between "verifiably false" and imprecise or obsolete information is blurred. It is also therefore necessary to define disinformation based on the intention of the author - economic gain or deception of the public. The fact that the intention of the author is significant also protects against governments classifying unwelcome information as disinformation. This must be prevented at all costs.

The fact that the mandate of the West Balkan and South Task Forces is being expanded is appropriate because disinformation is also giving rise to ever greater problems in those regions. Thus, disinformation in North Africa can exacerbate the refugee crisis.

The development of a digital **network between national authorities facilitates the sharing of intelligence which facilitates efforts to combat disinformation.** The Rapid Alert System provided for this may help Member States to nip disinformation campaigns in the bud. The extent to which this will actually be the case depends on how Member States react to an alert.

The Code of Practice for platform operators is appropriate as online platforms, especially social media platforms, are major distribution channels for disinformation. **By relying on a voluntary obligation, the Code of Practice balances the interests of the Commission and the technical and economic possibilities of platform operators.** The fact that online platforms are to prioritise credible information may limit the spread of disinformation. Thus, disinformation on Facebook - having been flagged as such by a fact-checker - will be displayed to users less often. What is problematic, however, is the fact that news agencies also work for platforms as fact-checkers. This may jeopardise the independence of news agencies. The closure of fake accounts is also appropriate as such accounts are often set up exclusively for the purpose of spreading disinformation.

By supporting the development of a European network of fact-checkers and academic researchers, the Commission is ensuring that fact-checkers can deploy their resources more efficiently. This makes it possible to combat disinformation more efficiently and effectively, especially on social media, e.g. by showing users before they forward information such as an image, that fact-checkers doubt its authenticity. With the huge amount of disinformation, however, fact-checkers, even where they are linked by extensive networks, can only examine a fraction of the messages.

It is also very important to raise public awareness about the phenomenon of disinformation - especially in social media - and thus increase people's resilience to disinformation.

Centrum für
Europäische Politik

Legal Assessment

Legislative Competency

The Action Plan affects various areas of EU competence that are all of equal importance.

Pillar 1 can be based on the EU's Common Foreign and Security Policy (CFSP). This covers all areas of foreign policy including all "questions relating to the security" of the EU [Art. 24 (1) TEU]. Thus, the expansion of EU capacity for combating and gathering disinformation from abroad is also included because disinformation, such as propaganda, can jeopardise the integrity of the EU. The EU is also pursuing a "good neighbourliness" policy with third countries and contributes to their development [Art. 8 EUV; Art. 209, Art. 212 (1) TFEU]; combating disinformation e.g. by supporting independent media, contributes to this by rationalising discussions and decisions.

Under Pillar 2, the EU can also work towards greater coordination in combating disinformation because it is obliged to communicate its activities and decisions to the public [Art. 15 (1) TFEU] and ensure public discourse based on the freedom of information, of the press and of the media [derived from Art. 11 CFR] which also includes correcting and raising public awareness of disinformation about the EU. Coordination between the EU and Member States in this regard can be based on the principle of sincere cooperation [Art. 4 (3) TEU]. Insofar as EU law is affected by disinformation, the EU can support Member States - such as via a "Rapid Alert System" - with their counter measures by facilitating the sharing of information [Art. 197 (2) TFEU].

Under Pillar 3, the EU can also reach agreements with online platforms in order to take action against disinformation in the internal market [Art. 114 TFEU].

Under Pillar 4, the EU can provide funds for cross-border collaboration [Art. 172 TFEU; cf. Schröder in: Streinz, EUV/AEUV, 3rd Edition, Art. 170 para. 6] as well as support, additional to that from the Member States, for research on disinformation [Art. 4 (3), Art. 182 (3) TFEU].

Subsidiarity

This is unproblematic for Pillars 1, 2 - because cooperation between Member States should be voluntary - and 3. Support for research projects under Pillar 4 must also satisfy the principle of subsidiarity in the individual case [cf. Ruffert in: Calliess/Ruffert, TEU/TFEU, 5th Edition, Art. 180, para. 3].

Proportionality with Respect to Member States

Unproblematic because no legal obligations are created.

Compatibility with EU Law in other respects

The Action Plan must be measured against Art. 11 CFR. This states that freedom of the media, freedom of expression and the freedom to "receive and impart information and ideas without interference by public authority" are protected (Freedom of expression and information). The latter also covers incorrect information [cf. Augsberg in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, 7th Edition, Art. 11 CFR para. 6]. Pillars 1, 2 and 4 are thus unproblematic. This would also apply to any strictly voluntary code of practice under Pillar 3.

The Commission's threat to turn the Code of Practice into law if it is not adequately complied with **is in breach of the freedom of the media**, upon which online platforms can also rely because they inter alia edit content for an indefinite number of people [cf. Jarass, Charta der GR, 3rd Edition, Art. 11 para. 17]. This is because the Commission is applying pressure for implementation - e.g. when it comes to editing and prioritising the displayed information - which ultimately means the Code of Practice is only voluntary in a formal sense. In addition, there is interference in the freedom of expression in that opinions, ideas etc., that are more effectively distributed via bots, must be designated as such and are therefore no longer free to be expressed in any form. Although such interference ultimately serves public safety and order and are justified [cf. Jarass, Charta der GR, 3rd Edition, Art. 11 para. 31], such restrictions must be specified by law [Art. 52 (1) CFR]. The Code of Practice, whose voluntary nature is in doubt, fails to meet this condition.

Conclusion

The development of a network between national authorities facilitates the sharing of intelligence which facilitates efforts to combat disinformation. By relying on a voluntary obligation, the Code of Practice balances the interests of the Commission and the technical and economic possibilities of platform operators. The Commission's threat to turn the Code of Practice into law violates the freedom of the media.