European Parliament
2014-2019

TEXTS ADOPTED
Provisional edition

P8_TA-PROV(2019)0187

Follow up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda against it by third parties

European Parliament recommendation of 13 March 2019 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 (2018/2115(INI))

The European Parliament,

– having regard to the European Council conclusions of 28 June and 18 October 2018,

– having regard to the Commission communication of 26 April 2018 entitled 'Tackling online disinformation: a European Approach' (COM(2018)0236),

– having regard to EU-wide Code of Practice on Disinformation published on 26 September 2018,

– having regard to its resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties[1],

– having regard to the Joint Communication by the High Representative of the Union for Foreign Affairs and Security Policy and the Commission of 6 April 2016 entitled 'Joint framework on countering hybrid threats: a European Union response' (JOIN(2016)0018),

– having regard to the Commission communication of 20 April 2016 on delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union (COM(2016)0230),

– having regard to the European Endowment for Democracy feasibility study on Russian Language Media Initiatives in the Eastern Partnership and Beyond, entitled 'Bringing Plurality and Balance to the Russian Language Media Space',

– having regard to the report of the Vice-President of the Commission / High

[1] OJ C 224, 27.6.2018, p. 58.

Representative of the Union for Foreign Affairs and Security Policy (VP/HR) of 18 May 2015 entitled 'The European Union in a changing global environment – A more connected, contested and complex world', and to the ongoing work on a new EU Global Security Strategy,

– having regard to its recommendation of 15 November 2017 to the Council, the Commission and the EEAS on the Eastern Partnership, in the run-up to the November 2017 Summit[1],

– having regard to the Joint Communication by the High Representative of the Union for Foreign Affairs and Security Policy and the Commission to the European Parliament and the Council of 13 September 2017 entitled 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' (JOIN(2017)0450),

– having regard to the Joint Communication by the High Representative of the Union for Foreign Affairs and Security Policy and the Commission to the European Parliament and the Council of 7 June 2017 entitled 'A Strategic Approach to Resilience in the EU's external action' (JOIN(2017)0021),

– having regard to Article 19 of the Universal Declaration of Human Rights (UDHR), which protects the right of everyone to maintain an opinion without interference and to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any media,

– having regard to the Joint Declaration on EU-NATO Cooperation of 10 July 2018,

– having regard to the Joint Declaration of 3 March 2017 on Freedom of Expression and 'Fake News', Disinformation and Propaganda by the UN Special Rapporteur on Freedom of Opinion and Expression, the Organisation for Security and Cooperation in Europe (OSCE) Representative on Freedom of the Media, the Organisation of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information,

– having regard to the Report of 6 April 2018 of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,

– having regard to its recommendation of 29 November 2018 to the Council, the Commission and the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy on Defence of academic freedom in the EU's external action[2],

– having regard to the most recent Europol 'European Union Terrorism Situation and Trend Report' from 2018, which highlighted the increase in the activities of terrorist groups in cyberspace and their possible convergence with other criminal groups,

– having regard to the Joint Communication of 5 December 2018 by the High Representative of the Union for Foreign Affairs and Security Policy and the Commission to the European Parliament, the European Council, the European

---

1 OJ C 356, 4.10.2018, p. 130.

2 Texts adopted, P8_TA(2018)0483.

Economic and Social Committee and the Committee of the Regions entitled 'Action Plan against Disinformation' (JOIN(2018)0036) and the Commission's Report on the implementation of the Communication 'Tackling online disinformation: a European approach' (COM(2018)0794) of the same date,

– having regard to the work of the Transatlantic Commission on Election Integrity,

– having regard to the Santa Clara Principles on Transparency and Accountability of Content Moderation Practices,

– having regard to the EU Action Plan on Strategic Communication of 22 June 2015,

– having regard to Rule 113 of its Rules of Procedure,

– having regard to the report of the Committee on Foreign Affairs (A8-0031/2019),

1. Recommends the following to the Council and the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy:

State of play 2018 – Tackling hybrid warfare

(a) to stress 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; expresses its concern about deteriorating media freedoms and cases of journalists being targeted; notes that further steps should be taken with all the relevant stakeholders to guarantee the transparency of media ownership and media pluralism without enforcing a censorship scheme and to protect an enabling environment for a wide variety of information, ideas, a diverse media and civil society landscape, as well as efforts aimed at identifying and raising awareness about disinformation and propaganda; to involve all of the relevant stakeholders including the main press, journalists' and media associations in these processes; underlines the importance of a functioning system of public broadcasting, which sets the standard of how to provide impartial and objective information in compliance with the best practice and ethics of journalism;

(b) to consider 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, also covering targeted sanctions against those responsible for orchestrating and implementing these campaigns, the need for which was demonstrated in particular by the hostile actions of state and non-state actors in these areas;

(c) to consider that Daesh has been changing its tactics, shifting from websites to the encrypted messaging service popular with Islamist groups;

(d) to support not only the growing number of state institutions, think tanks and NGOs dealing with propaganda and disinformation, but also grassroots cyber activities; calls on the VP/HR and the Commission 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; to ensure that EU strategic communication becomes a matter of high priority on the European agenda and that the EU institutions and Member States work hand in hand on preventing such phenomena, while bearing in mind that disinformation and propaganda thrive in a polarised environment with falling levels of trust in the media;

(e) to urge the Member States that continue to deny the existence of disinformation and hostile propaganda, the main sources of disinformation in Europe and the impact disinformation and propaganda have on public opinion to recognise them, and to encourage these Member States to take proactive measures in order to counteract and debunk such propaganda, including the proven cases of espionage by third countries; to invite all Member States to evaluate the situation within their territory and make relevant investments in their own capacity to counter strategic communication by hostile third parties and to improve the ability of citizens to detect disinformation, as well as to encourage Member States to ensure an effective exchange of information on this matter; to call on European leaders who have still not devoted sufficient attention to this threat to recognise the imminent necessity of a strategic awakening in order to counter hostile information warfare;

(f) to urge the Member States 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;

(g) to encourage the Member States to ensure an effective exchange of information between all of their relevant authorities for tackling propaganda, manipulation and disinformation, including the cyber and information warfare;

(h) to raise awareness about Russia's disinformation campaigns, as this constitutes the main source of disinformation in Europe;

Types of misinformation, disinformation and propaganda targeting the EU and its neighbours

(i) to recognise the work done at various levels to identify the types of influence and tools used against the EU and its neighbourhood; to raise awareness about ongoing disinformation campaigns and to shift attention to in-depth analysis and research of their impact and effectiveness in order to develop measures to counteract them in a proactive and swift manner; to encourage the Member States to establish permanent structures to identify, prevent and counteract disinformation; underlines that disinformation campaigns are part of a broader strategy and are usually accompanied by other hostile activities and that in particular information warfare accompanying military offensives should be taken seriously and counteracted with determination, unity and strength;

(j) to warn about the impact of artificial intelligence (AI) and its rapid development in the dissemination of fake news, and notes with concern that AI will soon be able to independently create further AI capabilities; to commit significant funding therefore to research and development at the intersection of AI and information warfare in view of the rapidly growing capabilities of AI in the area of spreading

propaganda and disinformation, including by means of, *inter alia*, deep fake videos;

(k) to focus on the ongoing use of disinformation by authoritarian actors such as Iran, whose dissemination of fake news instigates and inflames further tensions in volatile conflict zones while simultaneously targeting European populations to hide nefarious intent; to urge Member States to counteract such actions by enhancing cooperation and utilising lessons learned by like-minded countries and NGOs;

(l) to focus on and adapt 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, manipulated sound, images or video, AI, online news portals and TV stations to disseminate the main narratives, especially by opinion formers and state controlled or funded institutions that deliver key messages and narratives appealing to authoritarian actors; strongly condemns 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 cyberattacks is constantly growing;

(m) to pay special attention to messages and content openly aimed at encouraging violence, racism, suicide attacks, recruitment of 'foreign fighters', various crimes or overt incitement to one or more of these activities;

Industry and social media

(n) while acknowledging a new investment of effort by social media companies to tackle disinformation, to pay special attention to the effective implementation of the EU Code of Practice on Disinformation, while also inviting EU neighbour and partner countries to sign up to the EU Code of Practice on Disinformation, as well as paying special attention to the new tactic of using encrypted messaging services and social media which, in spite of their efforts to the contrary, are considered the most common tool for spreading disinformation, hostile propaganda and content that incites hatred and violence;

(o) to regulate, together with the Member States, the actions of social media companies, messenger services and search engine providers and ensure their full transparency and, in particular, accountability, adopting an EU-wide approach, 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, and to hold the companies 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; urges Member States, candidate countries and associated countries to adopt effective and clear legislation that ensures the transparency of media ownership; to pay particular attention to the funding, transparency and objectives of NGOs with links to authoritarian states operating in the EU and within its partner countries;

(p) to make sure the industry and online platforms deliver on the commitments undertaken in the Code of Practice on Disinformation and effectively tackle the disinformation problem by: (i) ensuring transparency of political advertising based on effective due diligence checks of the identity of sponsors, (ii) taking decisive action against fake accounts active on their services, (iii) identifying the misuse of automated bots, and (iv) cooperating effectively with independent fact-checkers;

(q) to urge social media companies and messenger service providers to ensure full compliance with EU data protection law and other regulations, and to react in real time and cooperate closely with the competent authorities in all investigations into the alleged use of their platforms for hostile purposes, and to perform transparent audits of entities suspected of spreading misinformation; calls on technology companies 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; to urge social media companies to react urgently when suspicious content of a political nature is disseminated, particularly if it incites to hate or crime;

(r) to bear in mind that the banning of suspicious accounts may be seen as censorship, and therefore make sure that such actions are justified if they are prescribed by law and carried out transparently, in cooperation with the competent authorities and civil society in Member States and partner countries, and with full insight into the reasons for doing so, including by urging social media companies to provide clear notice to all users about what types of content are prohibited, and clear notice to each affected user about the reason for the removal of their content or the suspension of their account; calls for alignment of internal set by social media for their users with legal order of the country they operate in;

Best practices

(s) to continue 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; to draw attention to the technical progress in this field and share examples of best practice in the form of measures already taken by individual Member States, including performing a review of the functioning of National Approaches introduced by the Member States, while developing ways of fostering close cooperation with the United Kingdom after Brexit, and to work in cooperation with the intelligence community and allies such as the US and Canada, NATO and the EU Intelligence and Situation Centre (INTCEN);

(t) to pay special attention to enhancing investigatory efforts into the ongoing process of outsourcing propaganda and using a set of force multiplying tools by hostile third parties, as well as to the importance of not only debunking, exposing and enhancing attribution capabilities, but also ensuring the clear attribution of such attacks, including publicly naming the perpetrators, their sponsors and the goals they seek to achieve, as well as measuring the effects of these attacks on the targeted audience; to publicise all debunked cases of hostile propaganda

accompanied by means of a detailed factsheet in an effort to alert the public in a manner that reaches the audience targeted by the given case of hostile propaganda;

(u) to support and involve civil society, the expert community, private institutions, academia, grassroots cyber activists, the mainstream press, journalists' and media associations and the growing number of actors targeted and affected in the further enhancement of measures aimed at fact-checking and the exposing of disinformation, deepening of research, including in-depth studies and sociological research, and more effectively analysing information manipulation; to support professional journalism, investigative reporting and projects that work on exposing disinformation as well as hi-tech start-ups that create digital tools arming the audience against disinformation attacks; to highlight the importance and need for providing funding and education, including seminars and training courses in cooperation with Member States and civil society, such as an online media literacy library and learning centre, aimed at awareness-raising and tackling disinformation and increasing media literacy;

(v) to welcome the set of measures adopted by NATO aimed at countering new types of hybrid threat and a joint communication on EU-NATO cooperation on this matter; to call for the EU to ensure effective and swift implementation of these recommendations, also at Common Security and Defence Policy (CSDP) level;

European approach

(w) to welcome the establishment of the new EEAS Strategic Communication Task Forces consisting of experts with appropriate linguistic skills and knowledge, namely the Task Force for Western Balkans and the Task Force South for the countries in the Middle East, Northern Africa and the Gulf region, which have been tasked with ensuring coordinated and consistent EU communications in the regions and counteracting disinformation and propaganda against the EU;

(x) to acknowledge the tangible results achieved by the East StratCom Task Force, including the creation of euvsdisinfo.eu and the @EUmythbuster account on Twitter; underlines that since its creation, it has debunked over 4 000 cases of disinformation campaigns on a wide variety of subjects; to continue to support the joint efforts of the Commission and the EEAS and the EU's East StratCom Task Force after an analysis of its strengths, weaknesses and the improvements needed, including improving its capabilities to detect, analyse and expose disinformation by equipping the EEAS Strategic Communication Task Forces and EU Delegations in the neighbourhood with new staff, tools and skills, including new data analysis tools, the recruitment of additional data scientists and disinformation experts, as well as covering a wider range of sources and languages on the reach and impact of disinformation;

(y) to urgently turn the East StratCom Task Force into a fully-fledged unit or even a bigger structure within EEAS, and to support, through the forthcoming allocation of funding by the European Parliament, all three EEAS Strategic Communication Task Forces by providing them with adequate financial and personnel resources, which are still required, aimed at the significant increase of their potential, effectiveness, professionalism, institutional continuity and quality of work, as well

as safeguarding them against political meddling by officials and countries that back Russian disinformation;

(z) to address the current deficiencies in the East StratCom Task Force, including lack of regional expertise, a large turnover of staff and lack of institutional continuity, and to ensure adequate financial resources and an adequate organisational structure, as this is the only way to ensure full professionalism, effectiveness and results;

(aa) to invite Member States which have not done so already to assign their own seconded National Experts, ensuring that the experts engaged by the EU to counter disinformation are not politically biased or active participants in internal political disputes within the given country, to the three StratCom Task Forces; to also invite close partner countries to advise the task force on the tactics employed by common state and non-state adversaries, and to acknowledge the importance and necessity of better coordination within the EU;

(ab) to intensify the cooperation between the East StratCom Task Force and all the EU institutions, Member States and like-minded partners; to encourage the EU Representations inside the EU, and the EU Delegations outside the EU, in supporting the work of the East StratCom Task Force, Task Force South and Task Force for Western Balkans, including by sharing international experiences and best practices and providing translations of their publications in local languages; calls for more dedicated staff to work on strategic communication, in particular in EU Delegations in the Eastern and Southern neighbourhood and the Western Balkans;

(ac) to focus on the accession countries and partners in the EU neighbourhood by assisting them in their efforts to counteract hostile propaganda and disinformation activities and including experts from the third countries in the EU neighbourhood that are subjected to the same threats, as well as giving priority to the development of a long-term strategic approach and outreach towards Eastern Partnership countries in particular; to strengthen the capabilities of the EU Delegations abroad and the Commission Representations and the European Parliament Liaison Offices in Member States to develop local capacity to detect and expose disinformation and to communicate the EU's values and policies effectively and extend campaign-based communication and better coordinate and amplify positive narratives across the EU institutions and Member States; to consider the current proliferation and future threats of disinformation aiming to threaten the independence, sovereignty and territorial integrity of all Eastern Partnership countries within their internationally recognised borders; to give priority in particular to the development of a long-term strategic approach and outreach towards Eastern Partnership countries, focusing on people-to-people exchanges, and working with existing civil society networks that already represent a source of community-based resilience;

(ad) to prioritise strategic communications, and to carry out a periodical review of EU policy on this issue; to continue support for the work of the European Endowment for Democracy (EED) towards practical solutions to support and strengthen democratic, independent and diverse Russian-language media in the countries of the Eastern Partnership and beyond; to invite the Commission and all Member

States and like-minded countries to positively engage in and support this project; to pay attention to any international actor that currently behaves in a similar way;

(ae) to propose to the European Council that counteracting disinformation and hostile propaganda is given priority with sufficient resources and instruments to safeguard objective reporting and dissemination of information;

(af) to link existing national and local specialised centres, news media, think tanks, NGOs and other actors and institutions, in particular NATO, dealing with hybrid warfare into an EU-wide network that would help coordinate their actions and gather their findings; to assign adequate resources to this undertaking; stresses that this network should be open to like-minded partners of the EU, which could share their experiences of being targeted by and countering disinformation and hostile propaganda; to ensure effective and swift implementation of EU-NATO recommendations on countering new types of hybrid threat, also at CSDP level, and to introduce the topic of countering strategic propaganda into the curriculum of the European Security and Defence College and its network;

Safeguarding elections from hostile propaganda

(ag) to strongly condemn 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 to call on the affected Member States to urgently conduct thorough investigations into these hostile campaigns; is 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; to stress the ability of independent democratic societies to make their own sovereign political choices which is legitimate;

(ah) to invite the Member States and like-minded countries to share data about any foreign or internal interferences in electoral processes and exchange best practices on counteracting them in order to increase resilience to such interference;

(ai) to invite 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, and stresses that these laws should be adequately amended to enable Member States to effectively and proactively counteract such threats; in this regard commends initiatives such as the Swedish Civil Contingencies Agency; to support the EU-associated countries and the Western Balkans with best practices as well as human resources and technology to ensure robust defence of their electoral processes from malicious cyber, disinformation and propaganda activities emanating from Russia and other hostile actors;

(aj) to invite Member States to adapt their electoral rules on online campaigning, and to monitor and evaluate the transparency features in relation to political advertising introduced by the online platforms;

(ak) to propose 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;

(al) to take stock of initiatives such as the bipartisan Transatlantic Commission on Election Integrity, bringing together representatives from politics, technology, the media and business with the aim of securing electoral process from foreign interference;

2. Instructs its President to forward this recommendation to the Council, the Commission and the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy and, for information, to the EEAS and NATO, as well as the President, Government and Parliament of Russia.