

INGE report

Compromise amendments

Need for an EU coordinated strategy

COMP 1 EPP (426, 435), SD (429), RE (425, 432, 433), Greens (428), ECR (431), Left (430), 427

2. Calls on the Commission to propose, and the co-legislators and Member States to support, 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 **as well as** deterrence tools, enabling them to tackle all hybrid threats and attacks orchestrated by foreign **State or non-State actors**; considers that this strategy should be built on:

- 1 – common **terminologies and** definitions, **single methodology, evaluation**, and ex post impact assessment of the legislation adopted so far, **shared intelligence system** as well as understanding, **monitoring including early warnings**, and situational awareness of the issues at stake,

- 2 – concrete policies enabling resilience-building among EU citizens in line with democratic values **including through support to civil society**,

- 3 – appropriate disruption **and defence** capabilities, and

- 4 – diplomatic and deterrence responses, **including a EU toolbox for countering foreign interference and influence operations, including hybrid operations, with adequate measures, e.g. attribution and naming of the perpetrators, sanctions and countermeasures, and global partnership to exchange practices and promote international norms of responsible state behaviour**;

COMP 2 SD (441), RE (440, 443), Greens (439), ECR (704)

3. Underlines that all measures to prevent, detect, **attribute**, counter and **sanction** foreign interference must be designed in way that respects and promotes fundamental rights, including **the ability of EU citizens to communicate in a secure, anonymous and uncensored way, without undue interference from any foreign actors**;

COMP 3 EPP (448), SD (270, 449, 452, 454, 459, 510, 874, 1105), RE (455, 456, 992, 1018), ECR (450, 512), Greens (453, 885)

4. Considers that this strategy should be based on a risk-based, whole-of-society and whole-of-government approach, covering the following areas in particular:
 - a) building EU resilience through situational awareness, media **and information** literacy, **media pluralism, independent journalism** and education,
 - b) foreign interference using online platforms,
 - c) critical infrastructure and strategic sectors,

- c a) *foreign interference during electoral processes,*
- d) covert funding of political activities by foreign *actors and donors,*
- e) cybersecurity and resilience against cyberattacks,
- f) protection of EU *Member States,* institutions, *agencies, delegations and missions,*
- g) interference through global actors via elite capture, national diasporas, universities, *and cultural events*
- h) deterrence, *attributions* and collective **countermeasures including** sanctions,
- i) global cooperation and multilateralism;

COMP 4 EPP (464, 468), SD (462), RE (424, 463, 470, 483, 493), ECR (467), Left (465), 469

5. Calls, in particular, for the EU *and its Member States* to *boost* the resources and means allocated to bodies and organisations - *such as think tanks, fact-checkers - across Europe and globally,* tasked with monitoring and raising awareness of the severity of threats including disinformation; *highlights the crucial role of the EU in a broader strategic understanding; calls for strengthening the foresight capacity and interoperability of the EU and its Member States to ensure robust preparedness to predict, prevent and mitigate foreign information manipulation and interference,* to strengthen the protection of *their* strategic interests and infrastructure, and to *engage in multilateral cooperation and coordination to reach a common understanding on this issue in the relevant international fora; calls on the Foreign Affairs Council to discuss matters of foreign interference on a regular basis;*

COMP 5 RE (420, 423, 471, 475), Greens (474), 476

6. Is concerned about the overwhelming lack of awareness, *including among the broader public and government officials,* of the severity of the current threats posed by foreign authoritarian regimes *and other malicious actors* targeting all levels and sectors of European society, aimed at undermining *fundamental rights and* public authorities' legitimacy, deepening political and social fragmentation *and, in some instances, even posing life threatening harm to European citizens;*

COMP 6 SD (480), RE (478 first part¹)

7. Is concerned about the lack of *norms and* appropriate and sufficient measures to *attribute and respond to acts of foreign interference, resulting in* an attractive *calculus* for malicious actors *of low costs, low risk and a high reward,* since the risks of *facing retribution for their actions are currently* very low;

COMP 7 RE (485), Greens (484)

8. Urges the Commission to include, *where relevant,* a foreign information manipulation

¹ Second part of 478 under Sanctions subheading.

and interference perspective in the ex-ante impact assessment carried out before presenting new proposals ***with a view of mainstreaming the countering of foreign interference and information manipulation within EU policymaking; urges the EEAS and the Commission to perform regular resilience reviews and to assess the development of the threats and their impact on current legislation and policies;***

COMP 8 EPP (491, 500, 508), SD (1124), RE (488, 514), ECR (490), Greens (496-2nd part), 489

9. Calls on the Commission to analyse recent national ***institutions***, such as Australia's National Counter Foreign Interference Coordinator, Finland's Security Committee assisting the government and ministries, Sweden's Civil Contingencies Agency, new agency for psychological defence and National China Centre, France's new national agency Viginum, ***Lithuania's National Cyber Security Centre, as well as the Taiwan's interagency disinformation coordination taskforce*** to see ***what we can learn from these best practices and to what extent a similar idea*** could be implemented at EU level; ***invites the Commission to support the sharing of information and best practices among Member States in this regard; underlines the importance of proactive approach and instruments, including the strategic communications as a core activity for implementing the EU and the Member States' policies through words and actions; calls on the Commission to provide adequate data science training and to create a single monitoring body within the Commission on information manipulation;***

COMP 9 RE (497), Greens (496-1st part, 499, 501)

11. Calls on the Commission to set up a ***Commission task-force led by Ms Jourova, as Vice-President in charge of Values and Transparency*** dedicated to scrutinising existing legislation and policies to identify gaps that could be exploited by malicious actors and ***urges the Commission*** to close these gaps; stresses that this structure should cooperate with other EU institutions and Member States at national, regional and local level and facilitate the exchange of best practices; ***calls on the Commission and EEAS to consider the establishment of a well-resourced and independent European Centre for Interference Threats and Information Integrity, that should identify, analyse and document interference threats against the EU as a whole and information manipulation operations, increase situational awareness, develop a specialised knowledge hub through becoming a platform for coordination with civil society, the business sector, EU and national institutions, and raise public awareness, inter alia via regular reports on systemic threats; stresses that the tentative creation of a new independent and well-resourced European Centre for Interference Threats and Information Integrity should clarify and enhance the role of the EEAS StratCom division with its taskforces as strategic body of the EU's diplomatic service and prevent the overlap of activities; stresses that EEAS StratCom's mandate should be focused on strategically developing external policies to counter existing and emerging joint threats and to enhance engagement with international partners in this field; points out that EEAS StratCom could pursue this in close cooperation with a new European Centre for Interference Threats and Information Integrity and a new Commission Taskforce;***

COMP 10 RE (1095, 2nd part), Greens (503), Left (504), 502

12. ***Calls on EU Institutions and Member States to empower civil society to play an active role in countering foreign interference; calls on all levels and sectors of European society to set up systems to make organisations and citizens more resilient against foreign interference, to be able to detect attacks on time and to counter attacks as efficiently as possible, including through education and awareness-raising, within the EU framework of fundamental rights and in transparent and democratic way; points, in this context, to the Taiwanese best practices and whole-of-society approach; calls on decision-makers to provide civil society with appropriate tools and dedicated funds to study, expose and combat foreign influence;***

Building resilience through situational awareness, media literacy and education

COMP 11 EPP (639), RE (519 1st part), Greens (600), ECR (507)

13. Stresses that EU institutions and Member States need sound, robust ***and interlinked*** systems to detect, analyse, track and map incidents of foreign state and non-state actors trying to interfere in democratic processes in order to develop situational awareness and a clear understanding of the type of behaviour that the EU and its Member States need to deter and address; ***calls for regular sociological research and polling to monitor resilience and media literacy as well as to understand public support and perceptions of the most common disinformation narratives;***

COMP 12 EPP (525), RE (523, 524, 526)

15. Underlines that it is necessary to develop a common methodology for developing situational awareness, ***early warning and threat assessment***, collecting evidence ***systematically*** and for ***timely*** detection of manipulation of the information environment, as well as ***developing*** standards for technical attribution, ***for example on content authenticity, in order to ensure an effective response;***

COMP 13 RE (530, 531), ECR (532), Left (529)

16. Stresses the need for the EU, in cooperation with Member States and ***working multilaterally in the relevant international fora***, to develop a conceptual definition of the interference threats ***faced by the EU***; underlines that this definition needs to reflect the tactics, techniques, procedures ***and tools used*** to describe the patterns of behaviour of the ***state and non-state*** threat actors that we see today; ***urges the Commission to involve the Fundamental Rights Agency (FRA) to ensure that there are no discriminatory or inequitable concepts or biases embedded in any conceptual definitions;***

COMP 14 EPP (535, 558, 1007), SD (528), Greens (538)

17. ***Underlines that public diplomacy and strategic communication are essential parts of the EU's external relations and the protection of the EU's democratic values***, calls for the EU institutions to further develop ***and boost*** the important work of the European External Action Service (EEAS) StratCom division, with its taskforces, EU Intelligence and Situation Centre (EU INTCEN) and Hybrid Fusion Cell, the ***EU Military Staff Intelligence Directorate***, the Rapid Alert System, the established cooperation at administrative level among the EEAS, the Commission and Parliament, the Commission-led network against disinformation, Parliament's administrative taskforce

against disinformation, and the ongoing cooperation with NATO, G7, civil society and private industry when it comes to cooperating on intelligence, analysis, the sharing of best practices and raising awareness about foreign information manipulation and interference; **welcomes the European Court of Auditors' Special Report 09/2021 entitled 'Disinformation affecting the EU: tackled but not tamed'; calls on EEAS and Commission to publish a detailed timeline for the implementation of ECA's recommendations;**

COMP 15 EPP (540, 542), RE (541)

18. Underlines the need to strengthen **permanent** monitoring efforts **while reinforcing them** well ahead of elections, **referenda** or other important political processes **across Europe;**

COMP 16 EPP (548, 550, 561), SD (549), RE (545, 551), Greens (546), Left (547)

19. Calls on Member States to make full use of these resources by sharing relevant intelligence to **EU INTCEN** and **enhance their participation** in the Rapid Alert System; is of the opinion that analysis and intelligence cooperation **within EU and with NATO** needs to be strengthened even **more while making it more transparent and democratically accountable, including by sharing information with Parliament;**

COMP 17 EPP (556, 557), SD (528), RE (554, 555)

20. Welcomes Commission President von der Leyen's idea of establishing a Joint Situational Awareness Centre **to improve strategic foresight and the EU's open strategic autonomy**, while expecting further clarification of its set-up and mission; underlines that such a centre would require active cooperation with **relevant** services of the Commission, the EEAS, the Council, Parliament **and national authorities;** **reiterates, however, the importance of avoiding duplication and overlap with existing EU structures;**

COMP 18 EPP (535, 561), SD (505), RE (436, 536, 566, 569)

21. Recalls the need to equip the EEAS with a **strengthened and clearly defined** mandate and the necessary resources **for the Strategic Communications and Information Analysis Division** to monitor and address information manipulation and interference beyond the **foreign sources** currently covered by the three taskforces and **to aim for a broader geographic coverage** by applying a risk-based approach; calls urgently for the deployment of adequate capabilities by the EEAS in order to address information manipulation and interference emanating from China, **notably by setting up a dedicated Far East team;** stresses further the need to significantly boost expertise and language capacity with regard to China and other strategically important regions, in the EEAS, **in the Member States**, and the EU institutions in general;

COMP 19 EPP (599, 574), RE (572, 575, 580, 620), Greens (571), ECR (578, 579), Left (576)

22. Stresses the importance of **broadly distributed, competitive, pluralistic media**, independent journalists, fact-checkers, researchers and **a strong public service media**, for a lively and free democratic debate; welcomes initiatives to bring together, train and

otherwise support organisations of independent journalists, fact-checkers and researchers all over Europe, and particularly in the regions most at risk, such as the European Digital Media Observatory *and the European Endowment for Democracy*; *therefore deeply regrets that the this observatory does not cover the Baltic States*; *welcomes as well initiatives aiming at establishing journalism and fact-checking trustworthiness indicators, that are easy to recognise, such as the one initiated by Reporters Without Borders*; *calls on Commission to counter monopolistic mass-media ownership*;

COMP 20 EPP (426, 574, 581, 592, 609), RE (590, 591, 608, 616), Greens (588), NI (595)

24. Calls *on the EU and the Member States to dedicate EU* public funding sources for independent fact-checkers, researchers, quality and *investigative* media and journalists, and NGOs *researching and investigating* information manipulation and interference, promoting media, *digital and information* literacy, and other means to empower citizens, and researching how to meaningfully measure the effectiveness of media, *digital and information* literacy training, awareness-raising, debunking and strategic communication;

COMP 21 EPP (598), SD (648), RE (585, 597, 618), ECR (587, 589, 596), NI (577)

- 24a *Calls for measures to strengthen professional and pluralistic media, ensuring that publishers receive a fair income for use of their content on the internet*; underlines that several countries around the globe are taking steps to ensure that the media have adequate financial resources; *reiterates its call for the creation of a permanent EU news media fund and* welcomes, in this regard *the NEWS initiative*, including the new funding possibilities for the media sector, media *and information* literacy in the 2021-2027 Creative Europe programme; *notes, however, that funding streams may create dependencies or have an impact on the independence of media*; *highlights in this regard the importance of transparency of media financing*; *believes that public disclosure of information on who owns, donates to, controls or provides content to media outlets and pays for journalistic content is needed to protect media pluralism*;

COMP 22 EPP (602, 605), RE (522, 601, 603)

25. Underlines the need to *consolidate* analysis, incident reports and *intelligence-based public threat assessments* with regard to information manipulation and interference *and make it* available to the public; therefore suggests the creation of a *EU-wide database on incidents of foreign interference reported by EU and Member States' authorities*; *underlines that information on these incidents could be shared, when appropriate, with civil society organisations and the public*, in all EU languages;

COMP 23 EPP (615), SD (619), RE (519, 674), Greens (612), ECR (673), 611

26. Calls on all Member States to include media and digital literacy, as well as *education in democracy, fundamental rights, recent history and world affairs*, critical thinking and public participation, in their curricula, from early years to adult education, including training for teachers and researchers; *calls on the Commission and the Member States to increase support for historical education and research on how foreign interference and past totalitarianism has influenced society in general, and large democratic events more specifically*;

COMP 24 EPP (609, 627, 629), SD (628), RE (610, 630)

28. Underlines the need to raise awareness *in all layers of society about foreign* interference; welcomes the initiatives taken by the EEAS, the Commission and Parliament's administration, such as training and awareness-raising events for journalists, teachers, influencers, students, *senior citizens* and visitors, both offline and online, in Brussels and *across EU Member States*, and recommends that they be further developed;

COMP 25 EPP (631), ECR (632)

29. Calls on the Member States, the EU administration and civil society organisations to share best practices for media *and information* literacy training and awareness-raising, as requested in the Audiovisual Media Services Directive; calls on the Commission to organise these exchanges in cooperation with the Media Literacy Expert Group; *underlines that the revised Directive needs to be rapidly and properly implemented by the Member States*;

COMP 26 EPP (606), SD (617), Greens (637), ECR (636)

30. Calls for the EU and its Member States to implement *tailored*, awareness-raising and media *and information* literacy programmes *including for* diasporas and minorities, and calls on the Commission to set up a system for the easy sharing of material in minority languages, in order to reduce translation costs and reach out to as many people as possible; *calls upon regions and municipalities to take a leading role since it is important to reach out to the rural areas and across demographic groups*;

COMP 26A EPP (722), (SD 891, 1099), (RE 929, 933), (Greens (624, 714, 716, 942), 713, 715, 939

- 30a. *Underlines that an essential response to foreign interference attempts is to defend the main targeted groups it is aimed at; emphasises the need for targeted action, through a harmonised EU legal framework, against the spread of disinformation and hate speech on issues related to gender, LGBTIQ+, minorities, refugees; calls on the Commission to develop and implement strategies to hinder the financing of individuals and groups that actively spread or participate in information manipulation, frequently aimed against the previously mentioned targeted groups and topics to divide society; calls for positive communication campaigns on these issues and underlines the need for gender sensitive trainings*;

COMP 26B RE (933), Greens (714, 716), 713, 715

- 30b. *Recognises that gendered disinformation attacks and campaigns are often used as part of a broader political strategy to undermine equal participation in democratic processes, especially for women and LGBTIQ+ people; stresses that disinformation about LGBTIQ+ persons fuels hate, both online and offline, and threatens lives; calls for research on online disinformation to be carried out with an intersectional lens and for oversight of the changes platforms are making to respond to gendered disinformation campaigns online; calls for increased attention on gender-based*

disinformation through the creation of early warning systems through which gendered disinformation campaigns can be reported and identified;

COMP 27 EPP (644), RE (643)

32. Underlines the importance of strategic communication to counter the most common anti-democracy narratives; *calls for the improvement of the European Union strategic communication to increase its reach both towards its citizens but also abroad*; stresses that all democratic organisations need to defend democracy and *uphold the rule of law* and have a common responsibility to engage with citizens, using their preferred languages and platforms;

COMP 28 EPP (649, 654), SD (648), RE (651, 655, 659), Greens (647), ECR (520, 652, 656, 658)

33. Is *deeply* concerned about the spread of foreign state propaganda, *mainly* originating in Moscow and Beijing *as well as Ankara*, which is translated into local languages, for instance in RT-, Sputnik- *Anadolu-*, *CCTV-*, *Global Times-*, *Xinhua-*, *TRT World*, or Chinese Communist Party-sponsored media content disguised as journalism, and distributed with newspapers; *maintains that such channels cannot be considered real media and therefore should not enjoy rights and protection of democratic media*; is *equally* concerned about how these narratives have spread into *genuine* journalistic products; *underlines the need to raise awareness about Russia's and China's disinformation campaigns, which aim at challenging democratic values and divide the EU, as these constitute the main source of disinformation in Europe*; *calls on the Commission to initiate a study on minimum standards for media as a basis to possibly revoke licenses in cases of breaches*; *asks the Commission to integrate the findings of the study within upcoming legislation such as a possible Media Freedom Act*; *notes that foreign interference actors may falsely present themselves as journalists*; *believes that it should be possible in such cases to sanction that person or organization, such as by naming and shaming, blacklisting to press events or revocation of media accreditation*;

COMP 29 EPP (666, 672), RE (663, 664, 668, 669), Greens (671), ECR (662), Left (665), 670

34. Is deeply concerned about *attacks*, harassment, *violence* and threats against journalists, *human rights defenders and other persons exposing foreign interference, which may also undermine their independence*; calls on the Commission to swiftly submit concrete and ambitious proposals on the safety of *all these persons, including an anti-SLAPP instrument and economic, legal and diplomatic support*, as announced under the European Democracy Action Plan; *welcomes, in this regard, the Commission Recommendation of 16 September 2021 on ensuring the protection, safety and empowerment of journalists and other media professionals*; *calls on the Member States to effectively protect journalists and other media professionals with legislative and non-legislative tools*;

COMP 30 SD (159, 677), RE (676, 679), Greens (678)

36. *Calls on the Commission and the Member States to establish communication channels and set up platforms where companies, NGOs and individuals, including diaspora*

members, can report to when they fall victim to information manipulation or interference; calls on the Member States to support those who are victims of attacks *and those who are aware of attacks* or are being put under pressure;

Foreign interference using online platforms

COMP 31 RE (682, 719, 721) and original paragraph 40

- 37. Welcomes the proposed review of the Code of Practice on Disinformation and the proposals for a Digital Services Act, a Digital Markets Act and other measures linked to the European Democracy Action Plan *as potentially effective tools to tackle foreign interference*; recommends that the final reading of these texts take into account the aspects set out in the remainder of this section;

COMP 32 EPP (687, 691), RE (684, 688, 748) ECR (693, 774), 692

37. Stresses that freedom of expression must not be misinterpreted as freedom to engage in online activities that are illegal offline, such as harassment, *hate speech, racial discrimination, terrorism, violence*, espionage and threats; underlines that platforms need not only to abide by the law *of the country in which they operate*, but also to live up to their terms and conditions, *especially in view of harmful content online*; *calls on platforms to strengthen efforts to prevent the reappearance of illegal content that is identical to what has been identified as illegal and has been removed*;

COMP 33 EPP (702), SD (943), RE (697, 701), Greens (700)

38. Underlines the need, above all, *to continue studying the rise of disinformation and foreign interference online and for EU-wide legislation to ensure* significantly increased and *meaningful* transparency, *monitoring and accountability* as regards the operations conducted by online platforms and also access to data for legitimate access seekers; *in particular when dealing with algorithms and online advertisement*; *calls for social media companies to keep ad-libraries*;

COMP 34 EPP (709, 710, 712), SD (754, 798), RE (621, 733, 734, 737, 796) Left (706)

39. Calls for regulation *and actions* to oblige platforms, *especially those with a systemic risk on society*, to do their part to reduce information manipulation and interference, for instance by using labels that indicate the true authors behind accounts, *limiting the reach* of accounts regularly used to spread disinformation or that regularly break the terms and conditions of the platform, suspending *and if necessary, and based on clear legislation, deleting* inauthentic accounts used for coordinated interference campaigns or demonetising disinformation-spreading sites, *setting up mitigation measures for interference risks containing the effects of their algorithms, advertising models, recommender systems and artificial intelligence (AI) technologies and flagging disinformation content in both posts and comments*; *recalls the need for these measures to be implemented in a transparent and accountable way*;

COMP 35 EPP (690, 726), SD (801), RE (725, 784, 785), Greens (724, 760)

41. Calls for *full and effective implementation of the GDPR, which limits* the amount of data platforms can store about users and how long this data can be used, especially for platforms and applications using very private and/or sensitive data, such as messaging,

health, finance and dating apps and small discussion groups, ***calls for gatekeeper platforms to refrain from combining personal data with personal data from other services offered by the gatekeeper or with personal data from third-party services***, to make it equally easy to disagree as to agree to the storage and sharing of data and to ***allow users to choose whether to be targeted with other personalized advertising online; welcomes all efforts to ban micro-targeting techniques for political advertising, particularly but not limited to those based on sensitive personal data, such as ethnic origin, religious beliefs or sexual orientation, and asks the Commission to consider extending a ban on micro-targeting to issue-based advertising;***

COMP 36 RE (728, 730, 735) Greens (731)

42. Calls for binding EU rules to require platforms to ***cooperate with competent authorities to regularly test their systems and to identify, assess and mitigate risks of information manipulation and interference and vulnerabilities that using their services carries, including how the design and management of their services contribute to that risk; calls for binding EU rules to oblige platforms to set up systems to monitor how their services are used, such as real-time monitoring of the most trending and popular posts in a country-by-country overview;*** in order to detect information manipulation and interference and flag suspected interference to the authorities responsible, and to increase the costs for actors who make it possible to turn a blind eye to any such actions facilitated by their systems;

COMP 37 EPP (732, 807, 811), SD (753), RE (734)

- 42a. ***Calls on online platforms to commit adequate resources to prevent harmful foreign interference; as well as for better working conditions, psychological care and fair payment for content moderators; calls on large social media platforms to provide detailed and country-by-country reports on the resources devoted to in-country fact-checking, research activities, content moderation, including human and AI capacities in individual languages, and collaboration with local civil society; underlines the need for these platforms to step up their efforts aimed at addressing disinformation in smaller and less commercially profitable markets in the EU;***

COMP 38 EPP (694, 696, 705) SD (754), RE (728, 734) + part of original para 42

- 42b. ***Calls on the social media platforms to fully respect the equality of all EU citizens irrespective of the used language in the design of their services, tools and monitoring mechanisms as well as in measures for greater transparency and a safer online environment; stresses that this refers not only to all official national and regional languages, but also to the languages of sizeable diasporas within the EU; underlines that these services should also be accessible for people with hearing impairment;***

COMP 39 RE (703, 786)

- 42c. ***Calls for clear and readable labelling of deep-fakes, both for platform users and in the content metadata, to improve its traceability for researchers and fact-checkers; in this respect, welcomes the initiatives aiming at improving content authenticity and traceability, such as development of watermarks and authenticity standards, by means of introducing global standards;***

COMP 40 EPP (745)

43. Calls for the regulation of services offering social media manipulation tools and services, *such as boosting the reach of accounts or content using artificial engagement or inauthentic profiles*; underlines that this regulation needs to be based on a thorough assessment of current practices and the associated risks *and should prevent that these services can be used by malicious actors for political interference*;

COMP 41 EPP (738, 741, 744), RE (739, 743), Greens (740), ECR (742)

44. Stresses the need for transparency as regards the real natural or legal person behind online content and accounts *for those wishing to advertise*; calls on platforms to introduce mechanisms to detect and suspend *in particular inauthentic* accounts linked to coordinated influence operations; underlines that *these practices should not interfere with the ability to be anonymous online, which is of crucial importance to protect journalists, activists, marginalized communities and persons in vulnerable positions (e.g. whistle-blowers or dissidents and political opponents of autocratic regimes) and allow room for satirical and humorous accounts*;

COMP 42 RE (684, 746, 749), Greens (752), ECR (699,), Left (750)

45. Underlines that a greater responsibility to remove any content must not lead to the arbitrary removal of legal content; urges caution as regards entirely suspending the accounts of real individuals *or the mass-use of automated filters*; *notes with concern the arbitrary decisions of platforms to suppress accounts of elected officials*; *stresses that these accounts should only be struck down based on clear legislation based on our democratic values, which are translated into business policy and are enforced by independent democratic oversight*; *and that there must be a fully transparent process contemplating the right to appeal*;

COMP 43 EPP (540), RE (758, 759), Greens (756), ECR (757), Left (706)

46. Calls for binding rules to require platforms to create easily available *and effective* communication channels for people or organisations who want to report *illegal content, violation of the terms and conditions, disinformation or foreign* interference or manipulation, *where appropriate allowing accused individuals to respond before any restrictive action is taken*, and to put in place *impartial, transparent, fast and accessible referral or appeal* procedures, for victims of content posted online, *those who submitted a notice*, and individuals or organisations affected by the decision to label, restrict visibility to, disable access to or suspend accounts or to restrict access to advertising revenue; *recommends that social media platforms designate a specific contact point for each Member State and form task force teams for every important election in every Member State*;

COMP 44 EPP (763), SD (727, 917), RE (761, 762, 784), Greens (760), ID (695), ECR (764), NI (698)

47. Calls for *legislative rules to ensure transparency vis-à-vis the user and the general public*, such as obligating platforms to set up public and easily searchable archives of online advertisements *including targeting and who paid for it, moderated and deleted content, self-regulatory measures* and give *comprehensive and* meaningful access to

information about the design, use and impact of algorithms to ***national competent authorities***, vetted researchers affiliated with academic institutions, ***media***, civil society organisations and international organisations representing the public interest; ***believes that the metrics of these libraries should be harmonized to allow for cross-platform analysis and reduce the administrative burden for platforms;***

COMP 45 EPP (767, 768,), SD (773), RE (607, 770, 771, 783), Greens (766), Left (769)

48. Calls ***for an end of business models that rely on encouraging*** people to stay on platforms longer by feeding them engaging content; ***calls on legislative decision-makers and platforms*** to ensure, ***through the use of human moderators and a third party auditor*** that algorithms do not promote illegal, extremist, ***discriminatory*** or radicalising content, but rather offer users a plurality of perspectives and ***prioritize and promote facts and science-based contents especially on important social issues such as public health or climate change;*** ***considers that engagement-based and addictive ranking systems pose a systemic threat to our society;*** ***calls on Commission to address the issue of current price-incentives where now highly targeted ads with divisive content often have much lower prices for the same amount of views than less targeted ads with socially integrative content;***

COMP 46 SD (707, 776), RE (777, 779)

49. Calls for algorithms to be modified in order ***to stop boosting*** content originating from inauthentic accounts and channels that artificially drive the spread of harmful foreign information manipulation; ***calls for algorithms to be modified so that they do not push divisive and anger-inducing content;*** ***stresses the need for the EU to put in place measures to legally bind the social media companies to eliminate such amplification of disinformation once detected to a maximum possible extent and that there has to be a consequence for platforms, if they do not comply with taking down disinformation;***

COMP 47 RE (778, 781), Left (782)

50. Stresses the need for ***an improved testing phase and*** a systematic review of the consequences of algorithms, ***including how they shape public discourse and influence political outcomes and how content is prioritized;*** underlines that such a review should also examine whether platforms can meet the guarantees promised in their respective terms and conditions and whether they ***have sufficient safeguards in place to prevent*** large-scale, coordinated inauthentic behaviours to manipulate the content shown on their platforms;

COMP 48 EPP (794), SD (799, 800), RE (791, 793, 803), Left (792)

51. Is alarmed by the ***average of €65 million in ad revenues that flow each year to approximately 1400 disinformation websites targeting European citizens^{1a};*** ***underlines that*** online advertisements, ***sometimes even by public institutions,*** end up on, and therefore finance, malicious websites promoting hate speech and disinformation, without the consent or even knowledge of the ***advertisers*** concerned; ***notes that five companies, including Google Ads, pay 97% of these ad revenues and are*** responsible for selecting publishers' websites listed in their ***inventory and so have the power to determine which content gets monetized and which not;*** ***considers it***

unacceptable that algorithms which distribute the advertising funds are a complete black box for the public; calls on the Commission to make use of the tools of competition policy and anti-trust law to ensure a functional market and break-up this monopoly; calls upon these actors to prevent disinformation websites from being funded by their ad services; congratulates organisations dedicated to raising awareness about this concerning issue; underlines that advertisers should have the right to know and decide where their advertisements are placed and which broker has processed their data; calls for the establishment of a mediation process, that allows advertisers to be refunded when ads are placed on websites that are promoting disinformation;

COMP 49 RE (729, 733, 802, 805, 817)

52. Underlines that the updated Code of Practice on Disinformation, the Digital Services Act, the Digital Markets Act and other measures linked to the European Democracy Action Plan will require an effective overview, assessment *and sanction* mechanism after their adoption, in order to evaluate their implementation at national and EU level on a regular basis and identify and remedy loopholes without delay *and to sanction misapplication of the commitments as well as inactions; calls in this respect for strong and resourceful Digital Services Coordinators in each Member State, as well as sufficient resources for the enforcement arm of the European Commission to execute the tasks it has been awarded by the DSA; furthermore, stresses the importance for online platforms to be subject to independent audits certified by the Commission; notes that to ensure independence of the auditor, the auditor cannot be funded by the individual platforms;*

COMP 50 RE (734, 806)

52a. *Calls in this respect for key performance indicators (KPIs) to be defined, by means of co-regulation, in order to have objective indicators to ensure verifiability of the actions taken by the platforms as well as their effects; underlines that these KPIs should include country specific-metrics such as the audience of disinformation, engagement (click-through rate, etc.), funding of in-country fact-checking or research activities, and indicators of the prevalence and strength of in-country civil society relationships;*

COMP 51 RE (720, 809)

52b. *Is deeply concerned by the lack of transparency in the revision of the Code of Practice on Disinformation, as the discussion remained largely preserved for the private sector and the European Commission; regrets that the European Parliament, in particular the INGE special committee, and some other key stakeholders were not properly consulted during the drafting of the review of the Code of Practice;*

COMP 52 SD (727), RE (802, 810, 812)

52c. *Deplores the continued self-regulatory nature of the Code since self-regulation is insufficient when it comes to protecting the public from attempts of interference and manipulation, is worried that the updated Code of Practice on Disinformation may not be able to provide an answer to the challenges ahead; is concerned by the strong reliance on the Guidance to strengthen the Code of Practice on the Commission's DSA proposal; calls for swift action to ensure that the Code of Practice incorporates*

binding commitments for the platforms to ensure EU's readiness before the next local, regional, national and European elections;

COMP 53 SD (799, 808), RE (787)

52d. *Calls for the EU to protect and encourage dialogue within the technology community and the exchange of information on the behaviour and strategies of social platforms; considers that only an open technological community can strengthen the public opinion against attacks, manipulation and interference; calls for an investigation the possibility of setting up a public-private Information Sharing and Analysis Centre (ISAC) for disinformation, where members would track, label and share threat information on disinformation content and their delivery agents according to a threat classification; believes that this could inform the EU Rapid Alert System and the G7 Mechanism and would also benefit smaller actors with less resources; calls also for an industry wide standard on ad services and online monetisation services to disinformation, for demonetizing harmful content which should be also used by online payment systems and e-commerce platforms and audited by a third party;*

Critical infrastructure and strategic sectors

COMP 60 EPP (821), SD (820), Greens (822)

53. Considers that, given its interconnected and cross-border nature, critical infrastructure is increasingly vulnerable to outside *interference* and believes that the framework currently in place should be revised; welcomes, therefore, the Commission's proposal for a new directive to enhance the resilience of critical entities providing essential services in the European Union;

COMP 61 SD (823, 825), RE (826, 827), Greens (828)

54. Recommends *that Member States maintain the prerogative to identify critical entities, but coordination at European level is needed to:*

- a) strengthen the connection and communication channels used by multiple actors, including for the overall security of EU missions and operations,*
- b) support the competent authorities in Member States through the Critical Entities Resilience Group, ensuring a diverse participation of stakeholders, and notably the effective involvement of SMEs, civil society organisations and trade unions,*
- c) and promote the exchange of best practices not only among Member States but also, at regional and local level, including with the Western Balkans, and among owners and operators of critical infrastructure, including through inter-agency communication, in order to identify concerning developments at an early stage and develop adequate countermeasures,*
- d) implement a common strategy on responding to cyber-attacks on critical infrastructure;*

COMP 62 SD (832), RE (829, 831), Greens (833)

55. *Recommends* that the list of critical *entities* could be extended to include *digital* election infrastructure, *and education systems* given their crucial importance in

guaranteeing the *long-term* functioning *and stability* of the EU and its Member States, and that flexibility should be allowed when deciding on the addition to the list of new strategic sectors to be protected;

COMP 63 Greens (834)

56. Calls for an overarching EU approach to tackle issues of hybrid threats to election processes and to improve coordination and cooperation among Member States; calls on the Commission to critically assess dependence on platforms and the data infrastructure in the context of elections; believes there is a lack of democratic oversight over the private sector; *calls for more democratic oversight of platforms, including appropriate access to data and algorithms for competent authorities;*

COMP 64 RE (533, 841), Greens (840), Left (839)

57. Recommends *that the obligations flowing from* the proposed directive, *including the assessments of the EU-wide and country-by-country* threats, risks and vulnerabilities, *which should reflect the latest developments and be* conducted by the Joint Research Centre in conjunction with the EEAS's INTCEN; underlines the need *for sufficient resources for these institutions to provide the latest state-of-the-art analysis, with strong democratic oversight and should not preclude prior evaluation by the Fundamental Rights Agency (FRA) to ensure respect for fundamental rights;*

COMP 65 EPP (845, 848, 849), SD (847, 850, 853, 862), Greens (844), ECR (843), Left (842)

58. Believes that the EU and its Member States need to provide financing alternatives to *EU, Western Balkans candidate countries and other potential candidate countries, where FDIs have been used as a geopolitical tool by third countries to increase the leverage of the above mentioned countries,* to prevent large parts of their critical infrastructure from coming into the possession of *foreign countries and companies,* such as in the case of the port of Piraeus in Greece and as is currently happening with Chinese investments in undersea cables in the Baltic, Mediterranean and Arctic seas; therefore welcomes the FDI Screening Regulation as an important tool to coordinate the actions of Member States on foreign investments, and calls for a stronger regulatory framework, *and stronger enforcement of the framework,* to ensure *foreign investments with detrimental effect, as specified in the regulation, to the EU's security are blocked, and* that more competences in screening FDIs are transferred to EU institutions; *calls for the abolishment of the lowest bidder principle in governmental investment decisions; calls on all Member States without investment screening mechanisms to establish such measures;* believes that the framework should be better connected with independent analyses, *to map and assess FDI flows,* by national and EU institutes *with other relevant stakeholders, such as* think tanks; considers that it might also be appropriate to include other strategic sectors in the framework, such as *5G and other information and telecommunication technologies (ICTs),* so as to limit its dependency on high-risk suppliers; *underlines that this approach should apply equally to candidate and potential candidate countries;*

COMP 66 EPP (860), SD (824, 852, 857), RE (851, 855), Greens (854, 1063), ECR (856)

59. Believes that the EU faces more challenges as a result of its ***lack of investments in the past that has contributed towards its*** dependence on foreign suppliers of technology; ***recommends securing production and supply chains of critical infrastructure and critical material within the EU***; believes that the EU's move towards ***open*** strategic autonomy and digital sovereignty is important and the right way forward; ***stresses that the EU is expected to deploy new tools to strengthen its geopolitical position, including an anti-coercion instrument***; considers the European Chips Act announced by the Commission, to ensure that parts that are vital for the production of chips are manufactured ***within the EU***, an important step in limiting dependence on third countries such as China and the US; believes that investment in chip production must be made in a coordinated manner across the bloc ***and on the basis of a demand side analysis, and*** avoid a race to national public subsidies and fragment the single market; calls on the Commission, therefore, to set up a dedicated European Semiconductor Fund, ***that could support the creation of needed skilled workforce and compensate the higher establishment costs for manufacturing and design facilities in the EU***;

COMP 67 RE (865, 867), Greens (864), ECR (863, 866)

60. ***Calls for further*** development of ***European networks*** of data infrastructure and service providers with European security standards, ***such as GAIA-X, which is*** an important step in ***building viable alternatives to the existing*** service providers ***and towards an open, transparent and secure digital economy***; ***underlines the need to strengthen SMEs and avoid cartelisation of the cloud market***; ***recalls that data centres are critical infrastructures***; ***is concerned about the influence of third countries and their companies on the development of GAIA-X***;

COMP 68 RE (868, 869)

- 60 a. ***Underlines that the integrity, availability and confidentiality of public electronic communication networks, such as internet backbones and submarine communication cables are of vital security interest***; ***calls on the Commission and Member States to prevent sabotage and espionage on those communication networks and to promote the use of interoperable secure routing standards to ensure the integrity and robustness of electronic communication networks and services, also via the recent Global Gateway strategy***;

COMP 69 SD (857), RE (870, 871), ECR (873), Left (872)

61. Calls on the Commission to propose actions to build a secure, sustainable, ***and equitable*** supply of the raw materials used to produce ***critical components and technologies, including*** batteries and equipment, ***5G and subsequent technologies, and chemical and pharmaceutical products, while stressing the importance of global trade, international cooperation with full respect for worker's rights, the natural environment and with the enforcement of international social and sustainability standards as regards the use of resource***; ***recalls the need to grant the necessary funding to research and development in order to find appropriate substitutes in case of supply chain disruption***;

Foreign interference during electoral processes

COMP 70 SD (838, 875, 876, 884 1st-part)

61 a. *Calls for establishing the protection of the entire electoral process as a top European and national security issue, since free and fair elections are at the heart of the democratic process; calls on the Commission to develop a better response framework to counter foreign interferences in electoral processes, which among others should consist of direct communication channels with citizens;*

COMP 71 SD (877, 879, 880, 884 2nd-part), RE (1015)

61 b. *Highlights the necessity to foster societal resilience against disinformation during electoral processes, including with private and academic sectors, and to adopt a holistic approach in which these interferences should be tackled on a constant basis, from school education programmes to the technical integrity and reliability of the vote and through structural measures to tackle their hybrid nature; in particular, calls for a plan to prepare the European elections in 2024, which involves a strategy, training and awareness raising for European political parties and their staff, as well as enhanced security measures to prevent foreign interference;*

COMP 72 SD (881, 883)

61 c. *Believes that mis/disinformation through social media, has become an increasing problem to electoral integrity; considers that social media platforms should ensure implementing and guaranteeing the well-functioning of policies to protect the integrity of elections; is alarmed by the recent findings on private firms being employed by malicious actors to meddle in elections, seed false narratives and push viral conspiracies, mostly on social media; calls for an in-depth investigation on how to counter the "Disinformation for hire" phenomenon as it is growing more sophisticated and common in every part of the world;*

COMP 73 SD (837, 878, 1016, 1154)

61d. *Highlights the utmost importance of election observation missions to providing relevant information and issuing specific recommendations to make the electoral system more resilient and to help counter foreign interferences in electoral processes; calls to improve and strengthen electoral processes, electoral observation missions being a key instrument in this combat against the increasing use of unfair and rigged electoral processes by illiberal regimes looking for democratic appearance; stresses in this view the need to reassess and update the tools and methods of international election observation to face new trends and threats including the fight against fake electoral observers, the exchange of best practices with like-minded partners, as well as closer collaboration with pertinent international organizations such as the OSCE and CoE, and all relevant actors in the framework of the Declaration of Principles for International Election Observation (DoP) and the Code of Conduct for International Election Observers; stresses that the participation of MEPs to unauthorised election observation missions undermine the credibility and reputation of the European Parliament; welcomes and recommends the full enforcement the DEG procedure for "cases of individual unofficial election observation by Members of the European Parliament"*

(adopted on 13 December 2018) which allows for the exclusion of MEPs from Parliament's official election observation delegations for the duration of the mandate;

Covert funding of political activities by foreign actors and donors

COMP 74 EPP (889), RE (886, 887), Greens (890)

62. *Stresses that, while there is still a need for a better understanding of the effects of covert financing of political activities on, for example, anti-democratic tendencies in Europe, nevertheless underlines that foreign funding of political activities through covert operations represents a serious breach of the integrity of the democratic functioning of the EU and its Member States, in particular during election periods, and therefore violates the principle of free and fair elections, and that it should therefore be made illegal in all EU Member States to engage in any covert activity financed by a foreign actors that aims to influence the process of European or national politics; notes in this respect that countries such as Australia have implemented laws that illegalize foreign interference in politics;*

COMP 75 SD (893, 894, 1028)

- 62 a. *Condemns the connection and explicit complicity of extremist, populist, anti-European parties and certain other parties and individuals with attempts to interfere in the Union's democratic processes and is alarmed that these parties are used as the voice of foreign interference actors to legitimize their authoritarian governments; calls for full clarification of the political and economic relations between these parties and individuals and Russia; considers these relationships to be highly inappropriate and condemns complicity which, in pursuit of political objectives, can expose Europe and its Member States to attacks by foreign powers;*

COMP 76 EPP (896, 905), SD (897, 902, 907, 918, 941), RE (901, 903, 906, 908, 910, 914, 916, 931), Greens (898, 911, 913, 921), NI (904)

63/64 (merged).

Calls on the Member States to close especially all the following loopholes in further harmonising national regulations, and to implement a ban on foreign donations:

- a) *in-kind contributions from foreign actors to political parties, foundations, people who hold public office or elected officials, including financial loans from any legal or physical persons based outside the EU and EEA (except European voters), anonymous donations above a certain threshold, lack of spending limits for political campaigns which allows influence through large donations; believes that political individuals, actors or parties who have been offered and/or accepted a financial or in-kind contribution by a foreign actor must have the obligation to report this to the competent authorities ; this information should be reported back to the European level to allow for EU-wide monitoring;*
- b) *straw donors with domestic citizenship²: transparency on physical and legal*

² Person who donates someone else's money to a political party or candidate using their own name.

donors must be enforced through conformability statements attesting to the status of the donor, greater enforcement powers given to electoral commissions, ***donations from within the EU that exceed a certain minimum threshold should be registered in an official and public register and be linked to a natural person and setting a ceiling for donations from private and legal persons (and subsidies) to political parties;***

- c) shell companies and domestic subsidiaries of foreign parent companies³: shell companies should be prohibited and more robust requirements established in order to reveal the origins of funding through parent companies; ***funding and donations to political parties beyond a certain threshold shall be registered in a public and central register with an official name and address that can be linked to an existing person, that countries should collect; calls on the Commission to ensure that authorities in Member States have the right to investigate the origins of the funding to verify the information from the domestic subsidiary and to address the lack of sufficient data in national registers, especially in situations in which a network of shell companies is used;***
- d) non-profit organisations and third parties⁴, coordinated by foreign actors and created with a view to influencing electoral processes: more uniform rules and transparency should be considered across the EU for organisations aiming to finance political activities when seeking to directly influence electoral processes such as elections and referendum campaigns; ***such rules should not prevent non-profit organisations and third parties from receiving funding for issues campaigns; rules creating transparency of funding or donations will have to apply to political foundations as well;***
- e) online political advertisements, which are not subject to the rules on TV, radio and print advertising and are usually not regulated at ***the European level***: there is therefore a need to ***prohibit advertisements bought by actors coming from outside of the EU and the EEA and*** guarantee complete transparency with regard to the ***purchasing of online political advertisements by actors from within the EU; underlines the need*** to ensure much greater ***transparency and democratic*** accountability as to the use of algorithms; ***welcomes the announcement of a new*** legislative proposal on the transparency of sponsored political content ***by the Commission***, as proposed under the European Democracy Action Plan, which ***should aim to prevent a patchwork of 27 different national legislations on online political advertising and*** will guarantee ***that EU parties are able*** to campaign online ahead of the European elections ***while limiting the risk of foreign interference and exploring which of the rules, that political parties within single Member States and major social media platforms that voluntarily adopted, can be made rules for everyone in the EU; calls on EU Member States to update their national political advertisings rules, which have not kept pace with the steady evolution towards the digital medium as the primary mode of political communication; calls on Commission to propose how to***

³ This loophole covers two different realities: the shell companies, which do not pursue actual business activities and are nothing but vehicles for financial covering; and the domestic subsidiaries of foreign parent companies used to funnel money into politics.

⁴ Non-profits and third parties are not required to disclose the identity of their donors, but are allowed to finance political parties and candidates in several EU Member States.

democratically define issue-based political advertising to end a situation where private for profit platforms decide what is issue-based and what is not;

COMP 78 EPP (922, 926, 938), SD (920, 925), RE (923), Greens (921), NI (928)

65. Calls on the Commission, therefore, to ***conduct an analysis of covert funding in the EU and*** submit concrete proposals aimed at closing all loopholes allowing for the opaque financing of political parties ***and foundations or elected officials*** from third-country sources and to propose common EU standards that would apply to national electoral laws in all Member States; believes that Member States should aim to introduce ***clear transparency requirements on funding of political parties as well as*** a ban on donations to political parties ***and individual political actors*** from outside the EU and the European Economic Area (EEA), with the exception of ***European*** voters living outside the EU and the EEA ***and to establish a clear strategy for the sanctions system; urges the Commission and the Member States to establish an EU authority for financial controls to combat illicit financial practices and interference from Russia and other authoritarian regimes; underlines the need to ban donations or funding that use emerging technologies that are extremely difficult to trace; asks Member States and Commission to allocate more resources and stronger mandates to oversight agencies with a view of achieving better data quality;***

COMP 79 EPP (936), RE (934), Greens (935, 940)

66. Welcomes the ongoing revision of Regulation (EU, Euratom) No 1141/2014 on the statute and funding of European political parties and foundations; supports all efforts to achieve a greater level of transparency in the financing of the activities of European political parties and foundations, in particular ahead of the European elections of 2024, including a ban on all donations from outside the EU and anonymous sources, ***with the exception of the diaspora from EU Member States, and on donations from outside the EU that cannot be documented either through contract, service agreements or fees associated to European political party affiliation while allowing membership fees from national member parties outside of the EU and EEA to European political parties; urges European and national political parties to commit themselves to fighting foreign interference and combatting the spread of disinformation by becoming signatories to a Charter containing specific commitments in this respect;***
- 66a. ***Stresses that an implementation of many of the Group of Countries against Corruption (GRECO) of the Council of Europe's and the Venice Commission's recommendations would strengthen the immunity of Member States' and the Union's political system from foreign financial influence;***

Cybersecurity and resilience against cyberattacks

COMP 80 EPP (945, 947, 952), SD (991, 1003), RE (944, 946), Greens (949), ECR (950), NI (951), 948

67. Urges the EU institutions ***and the Member States*** to rapidly increase investments in the ***EU's*** strategic ***cyber*** capacities and capabilities ***to detect, expose and tackle foreign interference***, such as artificial intelligence, secured communication, and data and cloud infrastructure, in order to improve the ***EU's*** cybersecurity, ***whilst ensuring respect for fundamental rights;*** calls on the Commission to also invest more in

increasing the *EU's* digital knowledge and technical expertise so as to better understand the digital systems used across the *EU*; calls on the Commission to allocate additional resources, both human, *material* and financial, to *cyber threat analysis capabilities, namely, EEAS's INTCEN, and* the cybersecurity of both the EU institutions, *namely ENISA and CERT-EU*, and the Member States; *regrets the lack of cooperation and harmonisation on cybersecurity matters between Member States;*

COMP 81 SD (953, 971), RE (957, 968), Greens (958), ECR (970)

68. Welcomes the proposals by the Commission for a new cybersecurity strategy and a new directive on measures for a high common level of cybersecurity across the European Union, repealing Directive (EU) **2016/1148(NIS2)**⁸; recommends that the final outcome of the ongoing work on the proposal addresses the flaws of the 2018 NIS Directive, notably by strengthening security requirements, *enlarging the scope, creating a framework for European cooperation and information sharing, strengthening Member States cybersecurity capabilities, develop public-private cooperation*, introducing stricter enforcement requirements *and making cybersecurity a responsibility for the highest level in management for European entities that are vital for our society*; emphasises the importance of reaching a high common level of cybersecurity across all Member States so as to limit weak points in joint EU cybersecurity; *underlines the crucial need to ensure resilience of information systems and welcomes in this regard the Cyber Crises Liaison Organisation Network (CyCLONe); encourages the further promotion of the OSCE confidence-building measures for cyberspace;*

COMP 82 EPP (964), RE (962, 967)

69. *Welcomes the Commission's proposal in the NIS2 to carry out coordinated security risk assessments of critical supply chains, similar to its 5G EU toolbox*, so as to better take into account risks linked to, *for example* the use of software and hardware produced by companies under the control of foreign states; *calls on the Commission* to develop global **6G** standards and competition rules, in accordance with democratic values; calls on the Commission to promote exchanges between EU institutions and national authorities about the challenges, best practices and solutions related to the toolbox measures; believes that the EU should invest more in its capacities in the area of 5G and post-5G technologies in order to reduce dependencies on foreign suppliers;

COMP 83 EPP (952), SD (954, 973), RE (959, 969)

70. *Welcomes the announcement* of creating a Cyber Resilience Act that would complement a European Cyber Defence Policy, as cyber and defence are *closely related*; calls for more *investments in* European cyber defence capabilities and coordination; *recommends to foster cyber capability-building of our partners through EU Training Missions or civilian cyber missions; underlines the need to harmonize and standardize cyber related training and calls for structural EU funding in that area;*

COMP 84 EPP (978), SD (975), RE (979), Greens (974, 986)

71. Condemns the massive scale and illicit use of **NSO group's** Pegasus surveillance software by state entities, *such as Morocco, Saudi Arabia, Hungary, Poland, Bahrain, United Arab Emirates and Azerbaijan* against journalists, human rights defenders and politicians; recalls that Pegasus is only one of the many examples of *a program that is abused* by state entities *for illicit, mass surveillance purposes* against innocent citizens; *also condemns other state spying operations on European politicians; urges the Commission to draw up a list of illicit surveillance software and continuously update this list; calls on the EU and Member States to use this list in order to ensure full due human rights due diligence and proper vetting of exports of European surveillance technology and technical assistance, and exports to European Member States with a clear rule of law problem; additionally, calls for the establishment of a European Citizen's Lab that, similar to the Canadian one, comprising journalists, human rights experts and reverse malware engineering experts that would be able to discover and expose the unlawful use of software for illicit surveillance purposes;*

COMP 84A Greens (986)

71a. *Calls on the EU to adopt a robust regulatory framework in this field in the EU and on the international level; welcomes in this regard the rule of the US Commerce Department's Bureau of Industry and Security to blacklist the NSO Group prohibiting the company from receiving American technologies;*

COMP 84B Greens (985)

71b. *Expresses its concern that the EU is cooperating on judicial and law enforcement matters with third countries that have been using the Pegasus spyware and engaged with NSO group to spy upon European citizens; calls for additional safeguards and enhanced democratic scrutiny on such cooperation;*

COMP 84C SD (981)

71c. *Calls on the European Commission to review the European investments in NSO [Group Technologies], to adopt targeted measures on foreign states using software to spy on European citizens or persons benefitting from the refugee status in European countries;*

COMP 85 EPP (984), SD (975, 981), Greens (974, 985, 986)

73. Points out the urgent need to reinforce the legislative framework so as to hold accountable those who distribute, use and abuse such software for illicit and unauthorised purposes; refers, in particular, to the sanctions imposed on 21 June 2021 on Alexander Shatrov, CEO of a Belarusian company producing facial recognition software used by an authoritarian regime, *for example to identify political opposition protesters; calls on the Commission to prevent any use or funding in the EU of illegal surveillance technologies; calls on the EU and Member States to engage with third country governments to end repressive cybersecurity and counter-terrorism practices and legislation, under enhanced democratic scrutiny; calls for an investigation by the competent EU authorities into the unlawful use of spyware in the EU and export from the EU, and for repercussions for Member states and*

associated countries, including those participating in EU programmes, who have bought and used the spyware and from which it has been exported to illegally target journalists, human rights defenders, lawyers and politicians;

COMP 86 EPP (988), RE (987, 989), Greens (980, 990)

74. Calls for an ambitious revision of the ePrivacy Directive in order to strengthen the confidentiality of communications and of personal data when using electronic devices, without lowering the level of protection provided by the *e-Privacy Directive (Directive 2002/58/EC)*, and without prejudice to Member States' responsibility to safeguard national security; highlights that public authorities should be obliged to disclose vulnerabilities they find in IT devices; calls for the EU and Member States to further coordinate their actions based on the Directive on Attacks against Information Systems in order to ensure that illegal access to information systems and illegal interception are defined as criminal offences *and met with appropriate sanctions*; recalls that every breach of confidentiality for national security purposes must be carried out lawfully and for explicit and legitimate purposes in a democratic society, on the basis of strict necessity and proportionality, as required by the ECHR and the Court of Justice of the European Union;

Protection of EU Member States, institutions, agencies, delegations and missions

COMP 87 SD (972, 995), RE (993, 996, 997)

75. Underlines that the EU institutions, *bodies, agencies, delegations, missions and operations*' networks, buildings and staff *are* a target for all types of hybrid threats and attacks by foreign state actors and should, therefore, be properly protected, *with special attention paid to the EEAS's assets, premises and activities abroad and the safety of EU staff delegated to non-democratic countries with repressive regimes*; calls for a structured response to these threats by CSDP missions, as well as to provide more concrete support to those missions through strategic communication; acknowledges the constant increase in state-sponsored attacks against EU institutions, bodies and agencies, including against the European Medicines Agency (EMA), and Member States' institutions and national public authorities;

COMP 88 SD (1001), RE (1000), Greens (999, 1013), ECR (998)

76. Calls for a thorough *and periodical* review of *all* services, networks, equipment and hardware of EU institutions, bodies and agencies, *delegations, missions and operations in order to bolster their resilience to cybersecurity threats and exclude potentially dangerous programmes and devices, such as Kaspersky Lab*; urges the EU institutions and the Member States to ensure proper guidance and secure tools for staff; emphasises the need to raise awareness of the use of secure services and networks within institutions and administrations, *including while on missions*; notes *the trust and security advantages of open-source based network operating systems, which are widely used by allied military and government agencies*;

COMP 89 EPP (1004, 1005), SD (966)

77. Stresses the importance of *efficient, timely and close* coordination between different EU institutions, bodies and agencies specialised in cybersecurity, such as the

Computer Emergency Response Team for the EU institutions (CERT-EU), alongside the full development of its operational capabilities, as well as the EU Agency for Cybersecurity (ENISA) and the upcoming Joint Cyber Unit which will ensure a coordinated response to large-scale cybersecurity threats in the EU; welcomes the ongoing structured cooperation between CERT-EU and ENISA; **welcomes as well the establishment of the EU cyber intelligence working group within EU INTCEN to advance strategic intelligence cooperation**; appreciates the recent initiatives taken by the Secretaries-General of the EU institutions to develop common information and cybersecurity rules;

COMP 90 EPP (1006)

78. Looks forward to the Commission's two proposals for regulations setting up a normative framework for information security and cybersecurity in all EU institutions, bodies and agencies, and is of the opinion that these regulations should include **capacity and resilience building**; calls on the Commission and Member States to allocate additional funds and resources to the cybersecurity of the EU institutions in order to meet the challenges of a constantly evolving threat landscape;

COMP 91 SD (1017), RE (622, 1002, 1008, 1039), Greens (1013)

- 79a ***Calls for a thorough investigation of the reported cases of foreign infiltration of the staff of the EU institutions; calls for a review and potential revision of human resources procedures, including pre-recruitment screening, to close loopholes enabling infiltration by foreign infiltration; calls on Parliament's governing bodies to improve security clearance procedures for staff and tighten rules and checks for access to its premises to avoid that individuals closely linked with foreign interests can have access to confidential meetings and information; calls on Belgian authorities to review and update the domestic anti-espionage framework to enable effective detection, prosecution and sanctioning of offenders; calls for similar actions in the other Member States to protect the EU institutions and agencies on their soil;***

COMP 92 EPP (1009), RE (1008), Greens (1010, 1013)

80. Calls on all EU institutions to raise awareness among their staff through proper training and guidance in order to **prevent**, mitigate and address cyber, and non-cyber, security risks; calls for mandatory and regular security **and ICT** training for all staff **(including interns)** and MEPs; **calls for regular and dedicated mapping and risk assessments of foreign influence within the institutions**;

COMP 93 SD (1014), RE (1011), Greens (1013)

- 81 a. ***Calls for mandatory transparency rules for trips offered by foreign countries and entities to EU institutions officials, including MEPs, APAs and group advisors, as well as for national officials, including but not limited to: the name of the paying agents, the amount, the stated motives; reminds that such organised trips cannot be considered as Parliament's official delegations and calls for strict sanctions should this not be respected; stresses that informal friendship groups can undermine the work of the official bodies of the Parliament, as well as for its reputation and the***

coherence of its action; urges Parliament's governing bodies to increase the transparency and accountability of these groups, to enforce current rules, and to take necessary measures when these friendship groups are misused by third countries; asks Quaestors to develop and maintain an accessible and up-to-date register of friendship groups and declarations;

Interference through global actors via elite capture, national diasporas, universities, and cultural events

COMP 94: EPP (1022), SD (1026), RE (1021, 1024)

82. Condemns all types of elite capture and the technique of co-opting top-level civil servants and former EU politicians used by foreign companies with links to governments actively engaged in interference actions against the EU, and regrets the lack of tools and enforcement needed to prevent these practices; considers that disclosing confidential information acquired during public mandates or when performing civil servant functions, at the expense of the EU and its Member States' strategic interests, should *have legal consequences and accompanied with severe sanctions, including immediate dismissal and/or disqualification from future recruitment by the institutions; considers that declaration of income and property of such individuals should be made publicly available;*

COMP 95: EPP (1032), SD (1030, 1037), RE (1029), Greens (1031)

83. Calls on the Commission to encourage and coordinate actions against elite capture, such as complementing *and implementing unexceptional enforcement of* the cooling-off periods for EU Commissioners *and high-ranking EU civil servants* with a reporting duty after the period, *to end the practice of "revolving door"*, and structured rules to tackle elite capture at EU level; *calls on the Commission to evaluate whether existing cooling-off requirements are still fit for purpose; underlines that former European politicians and civil servants should alert that they are approached by a foreign state at a dedicated supervisory body and receive whistleblower's protection; calls all the Member States to apply and harmonise cooling-off periods for their political leadership and to ensure that they have measures and systems in place requiring public officials to declare their outside activities, employment, investments, assets and substantial gifts or benefits from which a conflict of interest may result;*

COMP 96: EPP (1049, 1050), RE (1098), Greens (1045), ECR (1048)

87. *Strongly condemns the efforts to instrumentalise minorities in EU Member States* by the Kremlin **in** implementing so-called compatriot policies, particularly in the Baltic states and the Eastern Neighbourhood countries, are part of the geopolitical strategy of Putin's regime whose aim is to divide societies in the EU, alongside the implementation of the concept of the 'Russian world', aimed at justifying expansionist actions by the regime; *notes that many Russian "private foundations", "private enterprises", "media organisations" and "NGOs" are either state-owned or have hidden ties with the Russian state; stresses that it is of detrimental importance when engaging in dialogue with Russian civil society to make a difference between those organisations which stay clear of Russian governmental influence and those that have links to the Kremlin; recalls that there is also evidence of Russian interference and manipulation in many other Western liberal democracies, as well as practical support for extremist*

forces and radical-minded entities in order to promote the destabilization of the Union; notes that Kremlin broadly uses culture, including popular music, audiovisual content and literature, as part of its disinformation ecosystem; deplors Russia's attempts not to fully recognise the history of Soviet crimes and instead introduce a new narrative about Russia;

COMP 97: EPP (1051), RE (1097)

87 a. *Is concerned by attempts of the Turkish government to influence people with Turkish roots with the aim to use the diaspora as a relay for Ankara's positions and to divide European societies, in particular via the Presidency for Turks Abroad and Related Communities (YTB); condemns Turkey's open attempts to use its diaspora in Europe in order to change the course of elections;*

COMP 98: SD (1053, 1054, 1055, 1056, 1058)

87b. *Condemns the efforts from Russia to exploit ethnic tensions in the Western Balkans to inflame conflicts and divide communities, which could lead to a destabilization of the whole region; is concerned that the Orthodox Church in countries like Serbia, Montenegro and Bosnia and Herzegovina, especially in its entity Republika Srpska, attempt to promote Russia as protector of traditional family values and fortify relations between state and church; is alarmed that Hungary and Serbia are helping China and Russia with their geopolitical objectives; recommends convening dialogues with Western Balkan civil society and the private sector to coordinate anti-disinformation efforts in the region, with an emphasis on research and analysis and the inclusion of regional expertise; calls on the Commission to build up the infrastructure to produce evidence-based responses to both short-term and long-term disinformation threats in the Western Balkans; calls on the EEAS to pivot to a more proactive stance, focusing on building the EU's credibility in the region, rather than defending it in expanding StratCom monitoring to focus on cross-border disinformation threats emanating from countries within and neighbouring the Western Balkans;*

COMP 99: RE (1062), Greens (1059)

88. *Is alarmed by the extraterritorial application of coercive measures stemming from Hong Kong's new National Security Law and China's Law on Countering Foreign Sanctions, combined with the extradition agreements that China enjoys with other countries, enabling China to implement large-scale deterrence actions against critical non-Chinese nationals, for example, in a recent case, against two Danish parliamentarians and the Chinese counter-sanctions against five MEPs, the Parliament's Subcommittee on Human Rights, three MPs from EU Member States, the Political and Security Committee of the Council of the EU, two European scholars and two European think tanks in Germany and Denmark; calls on all Member States to resist and refuse extradition and, where appropriate, offer appropriate protection for the individuals concerned to prevent potential human rights violations;*

COMP 100: SD (1068), RE (1065)

89. *Is worried about the number of European universities, schools and cultural centres*

engaged in partnerships with Chinese entities, including Confucius Institutes, which enable the theft of scientific knowledge and the exercise of strict control over all topics related to China in the field of research and teaching, thus constituting a violation of the constitutional protection of academic freedom and autonomy, and over the choices of cultural activities related to China; ***is worried that such actions might lead to a loss of knowledge on China-related issues, depriving the EU of the necessary competences; is concerned e.g. by the sponsoring, in 2014, of the China Library of the College of Europe by the State Council Information Office of the Chinese Government^{8a}; is deeply concerned about Chinese pressure and attempts to censor e.g. the museum of Nantes regarding the exhibition on Genghis Kahn initially planned for 2020⁵***;

COMP 101: SD (1077), RE (932, 1070, 1071, 1081), Greens (1074)

90. Condemns the decision taken by the Hungarian Government to open a Fudan University branch while, at the same time, closing the Central European University in Budapest; is concerned about the increasing financial dependence of European universities on China ***and other foreign States, because of the risk of sensitive data, technologies and research outcomes flowing to foreign States and the implications this dependence could have for academic freedom; stresses the importance of academic freedom to address disinformation and influence operations; encourages these institutions to furthermore conduct detailed vulnerability assessments before entering into new partnerships with foreign partners; stresses that academic staff should be trained to report covert funding or influence through a dedicated hotline and those coming forward should always receive whistle-blower protection***; calls on the Commission and Member States to ensure ***that research of geopolitical concern at European universities are funded by European funds***; calls on the Commission to propose legislation on increasing the transparency of the ***foreign*** financing of universities ***as well as NGOs and think-tanks***, such as through mandatory donation declarations, ***due diligence of their funding streams and disclosure of funding, in-kind contributions and subsidies by foreign parties***; ***calls on Member State authorities to adopt effective rules on foreign funding of higher education institutions, including strict ceilings and reporting requirements***;

COMP 101A: Greens (1083)

91. ***Notes*** the increasing number of Confucius Institutes established around the world, and in particular in Europe; remarks that the ‘Center for Language Education and Cooperation’, ***formerly known as Confucius Institutes Headquarter or Hanban (or Office of Chinese Language Council International), which is responsible for the Confucius Institutes program worldwide, is part of the Chinese Party-State’s propaganda system***; calls on Member States and the Commission to support independent Chinese language courses without the involvement of the Chinese state ***or affiliated organisations***; believes that the recently established National China Centre in Sweden could serve as an important ***example of how to increase independent China competency in Europe***;

COMP 102: RE (1085, 1086)

92. Considers, in addition, that Confucius Institutes serve as a lobbying platform for

⁵ <https://www.chateaunantes.fr/expositions/fils-du-ciel-et-des-steppes/>

Chinese economic interests and for the Chinese intelligence service and the recruitment of **agents and** spies; recalls that many universities have decided to terminate their cooperation with Confucius Institutes because of the risks of Chinese espionage and interference, as did the universities of Dusseldorf in 2016, Brussels (VUB and ULB) in 2019, and Hamburg in 2020, and all universities in Sweden; ***calls for more universities to reflect on their current cooperation to ensure they do not affect their academic freedom; calls on Member States to closely monitor teaching, research and other activities within the Confucius Institutes and, where alleged espionage or interference is substantiated by clear evidence, take enforcement action to safeguard European economic and political sovereignty, including through denial of funding or revocation of licences of associated institutes;***

COMP 103: EPP (1094), SD (1093), RE (1089), Greens (1092), ECR (1090, 1091)

93. Observes that foreign interference can also be pursued through influence in and ***instrumentalisation of*** in religious institutes, such as Russian influence in Orthodox churches, in particular in Serbia, Montenegro, ***Bosnia and Herzegovina, especially in its entity Republika Srpska, Georgia and partly in Ukraine,*** including sowing division among local populations, developing a biased writing of history and promoting an anti-EU agenda, Turkish ***government*** influence through mosques in France and Germany ***and Saudi Arabian influence through Salafi mosques across Europe promoting radical Islam;*** calls on the Commission and Member States to ensure better coordination on protecting religious institutes from foreign interference ***and to cap and increase the transparency of funding; calls on Member States to closely monitor activities in religious institutes and, where appropriate and supported by evidence, take action, including through denial of funding or revocation of licences of associated institutes;***

COMP 104: RE (1069, 1095 1st part, 1102, 1104)

- 93a. ***Calls upon the EEAS to [produce] a study into the prevalence and influence of malicious state actors in European think tanks, universities, religious organizations and media institutions; calls on all EU institutions and Member States to collaborate with and engage in systematic dialogue with stakeholders and experts to accurately map and monitor foreign influence in the cultural, academic and religious sphere; calls for greater content sharing between European national broadcasters, including those in neighbouring countries;***

COMP 105: RE (1101, 1103)

- 93b. ***Is concerned by reports on foreign interference efforts in European judicial systems; draws particular attention to the execution of Russian judgments by European courts against Kremlin opponents; calls on Member States to raise awareness among judicial staff and work with civil society to prevent abuse of international judicial cooperation and European tribunals and courts by foreign governments; calls upon the EEAS to commission a study into the prevalence and influence of foreign interference in European court proceedings; notes that based on this study, it may be necessary to propose changes to transparency and funding requirements around court proceedings;***

Deterrence, attributions and collective countermeasures including sanctions

COMP 106: EPP (1114), SD (956, 1115), RE (1116)

94. Considers that the sanctions regimes recently set up by the EU, such as the restrictive measures against cyberattacks threatening the Union and its Member States⁶ and the EU Global Human Rights Sanctions Regime⁷ (*EU Magnitsky Act*), adopted on 17 May 2019 and 7 December 2020 respectively, have demonstrated added value in providing the EU with valuable deterrence tools; ***calls on the Commission to come forward with a legislative proposal to adopt a new thematic sanctions regime to address serious acts of corruption***; recalls that the cyberattack and human rights sanctions regimes have been used twice, in 2020 and 2021 respectively; ***urges that the cyber sanctions regime become permanent and calls on Member States to fully share evidence and intelligence in order to feed into the establishment of cyber sanction lists***;

COMP 107: EPP (1122), SD (1123, 1138), RE (434, 478, 1110, 1111, 1121)

95. Calls for the EU and its Member States to take further measures against ***foreign interference, including large-scale disinformation campaigns, hybrid threats and hybrid warfare***, with full respect for the freedoms of expression and of information, including in the form of setting up a sanctions regime; ***this should include the introduction of cross-sectoral and asymmetric sanction framework, as well as diplomatic sanctions, travel bans, asset freezes and the stripping of EU residence permits on targeted foreign individuals and their family members associated with foreign interference attempts***, which should target ***as precisely as possible*** the decision-makers and bodies responsible for aggressive actions, ***avoiding a tit-for-at environment***, under Article 29 of the Treaty on European Union (TEU) and Article 215 of the Treaty on the Functioning of the European Union (restrictive measures) ***and firmly integrated within the Union's Common Foreign and Security Policy (CFSP) and Common Security and Defence Policy (CSDP) pillars***; ***calls on Member States to make foreign and domestic interference and disinformation a fixed point on the agenda of the Foreign Affairs Council***; ***calls on the EU to define what internationally wrongful act is and adopt minimum thresholds for the triggering of countermeasures as a result of this new definition, and should be accompanied by an impact assessment to provide legal certainty***; ***notes that the Council should be able to decide on sanctions related to foreign interference with a majority vote, rather than unanimity***; is of the opinion that countries engaged in foreign interference and information manipulation with the aim of destabilising the situation within the EU should pay the costs of their decisions and bear the economic and/or reputational and/or diplomatic consequences; ***calls on the Commission and the High Representative of the Union for Foreign and Security Policy to submit concrete proposals in this regard***;

COMP 108: Greens (1126), Left (1125)

96. Insists that, while aiming to preserve democratic processes, human rights and freedoms as defined in the Treaties, a sanctions regime must pay particular attention to the impacts on fundamental rights and freedoms of any sanctions imposed, in order to uphold respect for the Charter of Fundamental Rights, ***as well as being transparent regarding the grounds on which the decision to implement sanctions is taken***; ***stresses the need for greater clarity at EU level regarding the scope and impact of***

⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2019%3A129I%3ATOC>

⁷ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2020:410I:TOC>

sanctions on associated persons, such as EU nationals and companies;

COMP 109: EPP (1130), RE (1127, 1208), Left (1128), ECR (1119, 1129)

97. Considers that while the nature of these hybrid attacks varies, their danger to the European Union's *and Member States'* values, fundamental interests, security, independence and integrity, as well as to the consolidation of and support for democracy, the rule of law, human rights and the principles of international law, *fundamental freedoms*, may be substantial in terms of either the scale of the attacks, their nature or their cumulative effect; *welcomes that the European Democracy Action Plan foresees that Commission and the EEAS together develop a toolbox for foreign interference and influence operations, including hybrid operations and including the clear attributions of malicious attacks from third parties countries against the EU;*

COMP 110: SD (1118, 1139), RE (478, 1112, 1134, 1135),

100. Underlines that, in order to reinforce their impact, sanctions should be imposed collectively based, *when possible*, on coordination with like-minded partners, also with respect to other types of reactions to the attacks, possibly involving international organisations and formalised in an international agreement; *notes the important work done by NATO in the area of hybrid threats and recalls in this respect* the communiqué of the NATO meeting of 14 June 2021, where it was reaffirmed that a decision as to when a cyberattack would lead to the invocation of Article 5 of the NATO Treaty would be taken by the North Atlantic Council on a case-by-case basis, and that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack⁸; *stresses that the EU and NATO should adopt a more forward-looking and strategic approach towards hybrid threats focussed on the motives and objectives of adversaries, as well as clarify in which instances the EU is better equipped to deal with a threat as well as the comparative advantages of their capabilities; recalls that there are several EU Member States which are not members of NATO, which nevertheless cooperate with NATO, for instance through its Partnership for Peace (PfP) programme and Partnership Interoperability Initiative (PII), and therefore underlines that any EU-NATO cooperation must be without prejudice to the security and defence policy of the non-NATO EU Member States including those which have neutrality policies; stresses the importance of mutual assistance and solidarity in line with Article 42.7 TEU and Article 222 TFEU and calls for the EU to set up concrete scenarios of activation of these Articles in a hypothetical cyberattack scenario and calls the EU and all Member States to link the issue with the other aspects of their relations with States behind interference and disinformation campaigns, in particular Russia and China;*

Global cooperation and multilateralism

COMP 111 ECR (1141), Left (1140),

101. Acknowledges that many democratic countries over the world are facing similar destabilisation operations carried out by foreign *state and non-state actors;*

⁸ https://www.nato.int/cps/en/natohq/news_185000.htm

COMP 112 EPP (1147), SD (1148, 1157), RE (1150), Left (1149)

102. Highlights the need for global, ***multilateral*** cooperation between like-minded countries ***in relevant international fora*** on these issues of crucial importance, under the form of a partnership based on common understanding and shared definitions, with a view to establishing international norms and principles; ***underlines the importance of close cooperation with the US and other like-minded state for the modernisation of multilateral organisations; in that regard, welcomes the Summit for Democracy and expects this to result in concrete proposals and actions to tackle the greatest threats faced by democracies today through collective action;***

COMP 113 SD (1151, 1154, 1162, 1168)

103. Considers that, on the basis of common situational awareness, like-minded partners should exchange best practices and identify common responses, ***on global, but also on shared domestic challenges***, including collective sanctions, ***protection of human rights and democratic standards; calls for the EU to lead the debate on the legal implications of foreign interference and to promote common international definition and attribution rules and develop an international framework for responses to interferences in elections to set a Global Code of Practice for Free and Resilient Democratic Processes;***

COMP 114 EPP (1142, 1146), RE (1150), Left (1156)

104. Calls for the EU and its Member States to consider the right international formats that would allow for such a partnership and cooperation between like-minded partners; ***calls on the EU and its Member States to initiate a process at the UN level to adopt a Global Convention to promote and defend democracy, that establishes a common definition of foreign interference; calls on the EU to propose a global Democracy Defence Toolkit, to be included into the Convention, containing joint actions and sanctions to counter foreign interference;***

COMP 115 SD (1167), RE (1196), Greens (1161)

105. Welcomes the NATO statement of 14 June 2021, which recognises the increasing challenge posed by cyber, hybrid and other asymmetric threats, including disinformation campaigns, and by the malicious use of ever-more sophisticated emerging and disruptive technologies; ***welcomes the progress made on EU-NATO cooperation in the cyber defence field; welcomes Lithuania's establishment of the Regional Cyber Defence Centre involving the US and the Eastern Partnership countries; supports closer cooperation in cyber defence, in terms of information sharing and operational work, with partner countries; welcomes the discussions on multilateral export controls on cyber-surveillance items between the US and the EU in the context of the Trade and Technology Council;***

COMP 116 EPP (1173, 1175), RE (1170, 1174), Left (1172)

107. Underlines that global cooperation should be based on ***common values reflected in common projects***, involving international organisations such as the Organisation for Economic Co-operation and Development and UNESCO, and setting up democratic capacity-building ***and sustainable peace and security*** in countries facing similar

foreign *interference* threats; calls for the EU to establish a European Democratic Media Fund to support independent journalism in *(potential) enlargement and* European neighbourhood countries *and in candidate and potential candidate countries*; *highlights the practical needs, such as obtaining technical work equipment, regularly voiced by independent journalists from neighbouring countries*;

COMP 117 SD (1176), Greens (543)

107a. Emphasises the urgent need to address climate mis- and disinformation; welcomes the efforts at COP26 to adopt a universal definition and outline actions to address the matter; calls for building on models such as the Intergovernmental Panel on Climate Change to create a global code of conduct on disinformation, a process that would provide the basis for a 'Paris Agreement on Disinformation';

COMP 118 EPP (1155, 1178, 1181, 1189, 1190, 1198, 1202), SD (660, 1144, 1165, 1182, 1191), RE (1177, 1185, 1192), Greens (1180), ECR (1186, 1187), Left (1183), 562, 1184

108. Stresses the importance of *providing a clear perspective for candidate and potential candidate countries and of supporting partner- and neighbouring* countries, such as those in the Western Balkans, and Eastern and Southern Neighbourhoods of the EU, since *countries like* Russia, *Turkey and China are* trying to use these countries as an information manipulation and hybrid warfare laboratory, *aimed at undermining the EU*; *believes the US is an important partner in countering foreign interference, disinformation campaigns and hybrid threats in those regions*; *is worried in particular by the role played by Serbia and Hungary to widely spread disinformation to surrounding countries*; *underlines that the EU should support and engage with these countries, as provided in the NDICI-Global Europe regulation*; considers its actions can take the form of *promoting the EU value added and positive impact in the region*, financing projects aimed at ensuring media freedom, *strengthening civil society and the rule of law*, and *enhancing* cooperation on media, *digital and information literacy, while respecting their sovereignty*; *calls for increasing the EEAS capacity in this regard*;

COMP 119 Greens (1194), 1197

108a. Encourages the EU and its Member States to deepen cooperation with Taiwan in countering interference operations and disinformation campaigns from malign third countries, including the sharing of best practices, joint approaches to fostering media freedom and journalism, deepening cooperation on cybersecurity and cyber-threats, raising citizens' awareness and improving overall digital literacy among the population in order to strengthen the resilience of our democratic systems; *supports intensified cooperation between relevant European and Taiwanese government agencies, NGOs and think tanks in this field*;

COMP 120 EPP (1198), Renew (1199)

109. Calls for Parliament *to actively promote an EU narrative and* to play a leading role in promoting the exchange of information and to discuss best practices with partner parliaments across the globe, using its vast network of interparliamentary delegations, as well as the democracy initiatives and support activities coordinated by its

Democracy Support and Election Coordination Group; *underlines the importance of close cooperation with parliamentarians from third countries through tailor-made projects supporting the European perspective for candidate and potential candidate countries;*

COMP 121 RE (1204, 1205), Greens (1194, 1203), 562, 1143, 1197, 1206

110. Calls for the EEAS to strengthen the role of the EU delegations *and the EU CSDP missions* in third countries in order to reinforce their ability to *detect and* debunk disinformation campaigns orchestrated by foreign state actors *and fund education projects strengthening* democratic values *and fundamental rights; strongly recommends the creation of a “Strategic Communication Hub”, initiated by the EEAS, to establish structural cooperation on countering disinformation and foreign interference, which should be based in Taipei; in addition, calls on EU delegations to contribute to the EU’s fight against disinformation by translating relevant EU decisions, such as European Parliament urgency resolutions, in their posted country’s language;*

COMP 122 EPP (506, 561, 1209), SD (539, 1210)

111a. Calls for the creation of a permanent institutional arrangement in the European Parliament dedicated to the follow-up of these recommendations, to address foreign interference and disinformation in the EU in a systematic way beyond the current timeline of INGE; calls for an improved institutionalised exchange between the Commission, EEAS and the Parliament through this body;

RECITALS

Introduction

COMP 123: SD (65), Left (36)

B. whereas foreign interference, information manipulation and disinformation are an abuse of the fundamental freedoms of expression and information as laid down in Article 11 of the Charter of Fundamental Rights of the European Union and threaten these freedoms, as well as *undermine* democratic processes in the EU and its Member States, such as the holding of free and fair elections; *whereas the objective of foreign interference is the distortion and false representation of facts, to artificially inflate one-sided arguments, to discredit information to degrade the political discourse and ultimately undermine the confidence in the electoral system and therefore in the democratic process itself;*

COMP 124: EPP (40), SD (42), ECR (41), Left (39, 486)

C. whereas any action against foreign interference and information manipulation must itself respect the fundamental freedoms of expression and information; *whereas the EU Fundamental Rights Agency (FRA) has a key role in evaluating respect for fundamental rights, including Article 11 of the Charter of Fundamental Rights, in*

order to avoid disproportionate actions; whereas actors of foreign interference and information manipulation misuse those freedoms to their advantage and, therefore, it is vital to step up precautionary fight against foreign interference and information manipulation because democracy depends on people making informed decisions;

COMP 125: EPP (29, 32, 33, 47, 48), SD (35, 46, 67, 75), RE (31, 45, 1107), ECR (44, 49), Left (30)

- D. whereas evidence shows that malicious *and authoritarian* foreign *State and non-State* actors, *such as Russia, China and others*, use information manipulation and other interference tactics to interfere in democratic processes in the EU; whereas these attacks, *which are part of a hybrid warfare strategy and constitute a violation of international law*, mislead and deceive citizens *as well as impact their voting behaviour, amplify divisive debates, divide, polarize and exploit vulnerabilities of societies, promote hate speech*, worsen the situation of vulnerable groups *which are more likely to become victims of disinformation*, distort the integrity of democratic elections and referenda, and sow distrust in *national governments*, public authorities, *liberal democratic order and have the goal to destabilise European democracy and, therefore, constitute a serious threat to the EU security and sovereignty*

COMP 126: EPP (61, 513), SD (60, 66), RE (58), ID (404), ECR (59)

- E. whereas foreign interference tactics take, *among others*, the form of disinformation, the suppression of information, the manipulation of social media platforms, *their algorithms, terms and conditions* and advertising systems, cyberattacks, hack-and-leak operations *to gain access to voter information and interfere with the legitimacy of the electoral process*, threats against and the harassment of journalists, researchers, politicians and members of civil society organisations, covert donations and loans to political parties, campaigns *favouring specific candidates*, organisations and media outlets, fake or proxy media outlets and organisations, elite capture and co-optation, *“dirty” money*, fake personas *and identities*, pressure to self-censor, the abusive exploitation of historical, religious and cultural narratives, pressure on educational and cultural institutions, taking control of critical infrastructure, pressuring foreign nationals living in the EU, *instrumentalisation of migrants* and espionage; *whereas these tactics are often combined with each other;*

COMP 127: EPP (71), SD (69, 77), RE (54, 68, 70), ECR (72)

- Da. whereas foreign interference is a pattern of behaviour that threatens or negatively impacts values, *democratic* procedures, political processes, *security of States and citizens and capacity to cope with exceptional situations*; whereas such interference is manipulative in character, and conducted *and financed* in an intentional and coordinated manner; whereas those responsible for such interference, including their proxies within and outside their own territory, can be state or non-state actors *and foreign interference is frequently accompanied by political accomplices in the Member State who derive political and economic advantages from favouring foreign strategies*; whereas foreign actors’ use of domestic proxies and cooperation with domestic allies blurs the line between foreign and domestic interference;

COMP 128: EPP (64, 114, 175, 477)

Ea. *whereas information manipulation and spreading of disinformation can serve economic interests of state and non-state actors and their proxies as well as creating economic dependencies that can be exploited for political aims; whereas in a world of non-kinetic international competition, foreign interference can be a prime tool for destabilizing and weakening targeted counterparts, or boosting one's own competitive advantage through the establishment of channels of influence, supply chain dependencies, blackmail or coercion; whereas disinformation is causing direct and indirect economic damage that has not been systematically assessed;*

COMP 129: EPP (123), SD (79, 1166), RE (78), Left (81)

G. *whereas there is a need to agree within the EU on common and granular definitions and methodology to improve the shared understanding of the threats and develop appropriate EU standards for improved attribution and response; in this respect, welcomes the work made by the EEAS; whereas these definitions must guarantee imperviousness to external interference and respect for human rights; whereas cooperation with like-minded partners, in relevant international fora, on common definitions of foreign interference in order to establish international norms and standards is of utmost importance; whereas the EU should take the lead in establishing clear international rules for attribution of foreign interference;*

Need for a coordinated strategy against foreign interference

COMP 130: EPP (85, 86), RE (87), ECR (84)

H. *whereas foreign interference attempts across the world are increasing and becoming more systemic and sophisticated, relying on widespread use of Artificial Intelligence and eroding attributability;*

COMP 131: SD (89), RE (93), Greens (91), 90

I. *whereas it is the duty of the EU and its Member States to defend all citizens and infrastructure as well as their democratic systems from foreign interference attempts; whereas, however, the EU and its Member States appear to lack the appropriate and sufficient means to be able to better prevent, detect, attribute and counter and sanction these threats;*

COMP 132: EPP (96), SD (82, 97), RE (95)

J. *whereas there is a general lack of awareness among many policy-makers, and citizens in general, of the reality of these issues, which may unintentionally contribute to opening up further vulnerabilities; whereas the issue of disinformation campaigns have not been on the top of the agenda of European policymakers; whereas the hearings and work of INGE special committee contributed to public recognition and contextualisation of these issues and have successfully framed the European debate on foreign interference; whereas long-lasting foreign disinformation efforts have already contributed to the emergence of home-grown disinformation;*

COMP 133: SD (103), RE (100), ECR (102)

K. whereas the **transparent** monitoring of the state of foreign interference in real time by institutional bodies and independent **analysts and** fact-checkers, **effective coordination of their actions and exchange of information** is crucial so that appropriate action is taken not only to provide information about ongoing malicious attacks but also to counter them; **whereas similar attention is needed for the so-called mapping of society and identifying its most vulnerable and susceptible parts to foreign manipulation and disinformation and tackling the causes of those vulnerabilities;**

COMP 134: SD (107), ECR (106),

L. whereas the **first priority of the EU defence is** resilience **and preparedness** of EU citizens against foreign interference and information manipulation requires a long-term and whole-of-society approach **starting at the level of education and rising awareness about the problems at an early stage;**

COMP 135: EPP (110), SD (109), RE (111, 150), ECR 112

M. whereas it is necessary to cooperate and coordinate across administrative levels and sectors **among the Member States, at the EU level and with like-minded countries as well as with civil society and private sector**, to identify vulnerabilities, detect attacks and **neutralise** them; **whereas there is an urgent need to synchronise the perceptions of threats to national security;**

Building resilience through situational awareness, media and information literacy, media pluralism, independent journalism and education

COMP 136 EPP (122, 127), SD (213), RE (130), Greens (121), ECR (118), 120 and 2nd part of original recital O

N. whereas situational awareness, **robust democratic systems, strong rule of law, a vibrant civil society, early warning and threat assessment** are the first **steps** towards countering information manipulation and interference; whereas in spite of all the progress made in raising awareness **-about foreign interference**, many people, including policy-makers and civil servants working in the areas potentially targeted, are still unaware of the **potential** risks linked to foreign interference and how to **address** them;

COMP 137 EPP (126, 133), RE (132) ECR (125, 160)

O. whereas high-quality, sustainably **and transparently** financed and independent news media and professional journalism are essential for media freedom and pluralism and the rule of law, and are therefore a pillar of democracy **and the best antidote to disinformation; whereas some foreign actors take advantage of Western media freedom to spread disinformation;** whereas professional media and traditional journalism, as a quality information source, are facing challenging times in the digital era; **whereas quality journalism education and training inside and outside the EU is necessary in order to ensure valuable journalistic analyses and high editorial standards; whereas the EU needs to continue supporting journalism in the digital environment; whereas science-based communication should play an important role;**

COMP 138 EPP (131), Left (124)

Oa. *whereas editorially independent public service media is essential and irreplaceable in providing high-quality and impartial information service to the general public and shall be protected from malign capture and strengthened as a fundamental pillar of the fight against disinformation;*

COMP 139 RE (134, 136)

P. *whereas different stakeholders and institutions use different methodologies and definitions to analyse foreign interference – all with different degrees of comprehensibility, and whereas these differences can inhibit comparable monitoring, analysis and assessment of the threat level, which makes joint action more difficult; whereas there is a need for a EU definition and methodology to improve the common threat analysis;*

COMP 140 SD (135), RE (139, 140), ECR (138)

Q. *whereas there is a need to complement terminology that focuses on content, such as fake, **false or misleading** news, **misinformation** and disinformation, with terminology that centres on behaviour, in order to adequately **address** the problem; **whereas this terminology should be unified and carefully adhered;***

COMP 141 SD (144), RE (141, 169, 613), ECR (142, 154)

R. *whereas training in media and digital literacy and awareness-raising, **for both children and adults**, are important tools to make citizens more resilient against interference attempts in the information space **and avoid manipulation and polarization;** **whereas in general, societies with a high-level of media literacy are more resilient to foreign interference;** **whereas journalistic working methods such as constructive journalism could help strengthen trust in journalism among citizens;***

COMP 142 EPP (148), SD (149, 446, 527), RE (145), ECR (147)

S. *whereas information manipulation can take many forms, such as spreading disinformation **and completely false news**, distorting facts, **narratives** and representations of opinion, suppression of certain information or opinions, taking information out of context, **manipulating people's feelings, promoting hate speech**, promoting some opinions at the expenses of others, and harassing people to silence **and oppress** them; **whereas an aim of information manipulation is to create chaos to encourage a loss of trust by citizens in the old and new 'gatekeepers' of information;** **whereas there is a fine line between freedom of expression and the promotion of hate speech and disinformation that should not be misused;***

COMP 142a RE (146, 663),

Sa. *whereas Azerbaijan, China, Turkey and Russia, among others, have all targeted journalists and opponents in the European Union, such as the case of Azerbaijani blogger and opponent Mahammad Mirzali in Nantes or Turkish journalist Erk Acarer in Berlin;*

COMP 143 EPP (151, 182), SD (289), RE (173, 317), Greens (53, 57, 193, 218, 312), Left (291), 52, 56, 235, 314

Sb. *whereas there is concrete evidence that the EU's democratic processes are being targeted, and interfered with, by disinformation campaigns that challenge democratic ideals and fundamental rights; whereas disinformation related to topics, including but not limited to, gender, LGBTIQ+, sexual and reproductive health and rights, and minorities is a form of disinformation that threatens human rights, undermines digital and political rights, as well as the safety and security of its targets, and sows fraction and disunity among Member States; whereas during election campaigns female political candidates tend to be disproportionately targeted by sexist narratives, leading to the discouragement of women to take part in democratic processes; whereas the perpetrators of these disinformation campaigns, under the guise of promoting 'traditional' or 'conservative' values, form strategic alliances with local partners to gain access to local intelligence and have been reported to receive millions of euros in foreign funding*

COMP 144 EPP (157), SD (156), Renew (99, 445, 1195), Greens (153), ECR (155), 152

T. *whereas next to state institutions, journalism, opinion leaders and the private sector, each section of society and each individual have important roles to play to identify and stop the spread of disinformation and warn people in their environment who are at risk; whereas civil society, academia and journalists have already contributed strongly to raising public awareness and increasing societal resilience also with counterparts in partner countries;*

COMP 145 Greens (153), 152

Ta. *whereas civil society organisations representing minority voices and human rights organisations across Europe remain underfunded, despite playing a crucial role in raising awareness and countering disinformation; whereas civil society organisations should be adequately resourced to play their part in limiting the impact of foreign interference;*

COMP 146 EPP (161, 162)

U. *whereas it is important to have easy and timely access to fact-based information from reliable sources when disinformation starts to spread;*

COMP 147 EPP (166, 167, 544), SD (119, 164, 528, 680, 804), RE (582)

V. *whereas it is necessary to rapidly detect foreign interference attacks and attempts to manipulate the information sphere in order to counter them; whereas EU intelligence analysis and situational awareness is dependent on the willingness of Member States to share information; whereas the EC President proposed to consider setting up an EU Joint Situational Awareness Centre; whereas prevention and proactive measures including pre-bunking and a healthy information ecosystem are far more effective than subsequent fact-checking and debunking efforts, which show lower reach than the original disinformation; whereas the EU and its Member States currently lack sufficient capabilities to do that; whereas new AI-based analytical tools, such as Lithuanian Debunk.eu, could help detect attacks, share knowledge and inform the public;*

COMP 148 RE (170)

- W. whereas disinformation thrives ***in an environment of weak or fragmented national or EU-level narrative***, on polarised and emotional debates, exploiting weak points and biases among society and individuals, and whereas disinformation distorts the public debate around elections and other democratic processes and can make it difficult for citizens to make informed choices;

Foreign interference using online platforms

COMP 149 EPP (174, 177, 178, 181, 183, 765), SD (185), RE (176, 179, 188), ECR (180) and original recital X

- Y. whereas online platforms can be ***easily accessible and affordable*** tools for those engaging in information manipulation and other interference, such as hate and harassment, ***damaging the health and safety of our online communities***, silencing of opponents, espionage or spreading of disinformation; ***whereas their functioning has been proven to encourage polarized and extreme opinions at the expense of fact-based information; whereas platforms have their own interests and may not be neutral in processing information; whereas some online platforms greatly benefit from the system that amplifies division, extremism and polarization; whereas the online space has become equally important for our democracy as the physical space and therefore needs corresponding rules;***

COMP 150 EPP (197), SD (186, 187, 200) RE (88, 184, 199, 681), ECR (198)

- Z. ***whereas platforms have accelerated and exacerbated the spread of mis- and disinformation in an unprecedented and challenging way; whereas online platforms control the flow of information and advertising online, whereas platforms design and use algorithms to control these flows, and whereas platforms are not transparent, lack appropriate procedures to verify identity, use unclear and vague terminology and share very little or no information about the design, use and impacts of these algorithms; whereas the addictive component of online platform algorithms has created a serious public health problem that needs to be addressed; whereas online platforms should be responsible for the harmful effects of their services, as some platforms were aware of the flaws of their algorithms - in particular their role in spreading divisive content - and have failed to address them to maximise profit, as was revealed by whistle-blowers;***

COMP 151 EPP (192, 194), RE (55, 74, 165, 189, 191, 201), ID (387), ECR (196) and original recital Y

- Za. whereas ***there are*** interference and information manipulation campaigns directed at all the measures against the spread of COVID-19, including vaccination across the EU, and online platforms have ***failed to coordinate and contain them and may have even contributed to their spread; whereas such disinformation can be life-threatening when deterring people from being vaccinated or promoting false treatments; whereas the pandemic has exacerbated the systemic struggle between democracy and authoritarianism, prompting authoritarian state and non-state actors, such as China and Russia, to deploy a broad range of overt and covert instruments in their bid to destabilise their democratic counterparts; whereas the “Facebook Papers” have revealed the platform’s failure to tackle vaccine-related disinformation, including in the English language; whereas the situation is even worse for non-English vaccine-***

related disinformation; whereas this issue concerns all platforms;

COMP 152 EPP (202, 204, 206), SD (203, 208, 279), RE (219), ECR (207)

AA. whereas numerous vendors registered in the EU sell *inauthentic* likes, *followers* comments and shares to any actor wishing to artificially boost their visibility online; whereas it is impossible to identify legitimate uses of such services, while harmful uses include manipulating elections *and other democratic processes*, promoting scams, negative reviews of competitors' products, defrauding advertisers *and the creation of a fake public that is used to shape the conversation, for personal attacks and artificially inflate certain viewpoints that would otherwise get no attention* whereas foreign regimes, such as *Russia and China, are massively using these online tools to influence the public debate in European countries; whereas disinformation can destabilise European democracy;*

COMP 153 RE (209), Greens (210)

AB. whereas social platforms, digital devices and applications collect and store immense amounts of very detailed personal and often sensitive data about each user; whereas such data *can be used to predict behavioural tendencies, reinforce cognitive bias and orient decision-making; whereas such data is exploited for commercial purposes;* whereas data leaks happen repeatedly, *to the detriment of the security of victims of such leaks, and data can be sold on the black market;* whereas such databases could be goldmines for malicious actors wanting to target groups or individuals;

COMP 154 SD (212), Greens (211)

AC. whereas, *in general, platforms are designed to ensure that* opting not to share data is *nonintuitive*, cumbersome and time-consuming in comparison with opting to share data;

COMP 155 SD (215), RE (163, 216), Greens (217)

AD. whereas online platforms are integrated into most parts of our lives and *the information spread on platforms* can have a huge impact on our thinking and behaviour, for instance when it comes to voting preferences, *economic and social choices as well as choice of information and that these decisive choices of public importance are today in fact conditioned by the commercial interests of private companies;*

COMP 156 SD (186, 221, 224, 234), RE (220, 223), Left (222)

AE. whereas algorithm curation mechanisms *and other features of social media platforms are* engineered to maximise engagement; whereas these features are repeatedly reported to promote polarising, radicalising *and discriminatory* content and *keep users in likeminded circles; whereas this leads to a gradual radicalization of the platforms users as well as conditioning and polluting of collective discussion processes, rather than protecting democratic processes and individuals; whereas uncoordinated actions by platforms have led to discrepancies in their actions and let disinformation spreading between platforms; whereas the business model of making money through the spreading of polarising information and the design of the algorithms make platforms an easy target for manipulation by foreign hostile actors; whereas social*

media platforms could be designed differently so as to foster a healthier online public sphere;

COMP 157 RE (226), ECR (225)

AF. whereas *creation of deepfake of audio and audiovisual materials is getting increasingly easier with the advent of affordable and easy to use technologies, and the spread of the deepfake audio and video materials is an exponentially increasing problem; whereas currently however, 90% of research goes to the development of deepfakes and only 10% into their detection;*

COMP 158 SD (229), RE (228, 233), Greens (232)

AG. whereas self-regulation systems such as the 2018 Code of Practice on Disinformation have led to improvements; *whereas, however, relying on the goodwill of the platforms is not working nor effective and has produced little meaningful data on their overall impact; whereas, in addition, platforms took individual measures varying in degree and effect, leading to backdoors allowing content to continue spreading elsewhere while being taken down ; whereas there needs to be clear set of rules and sanctions in order for the Code of Practice to have sufficient effect on the online environment;*

COMP 159 EPP (230), SD (236, 882)

AGb. whereas the European Democracy Action Plan aims to strengthen the 2018 Code of Practice and together with the Digital Services Act constitutes a step away from the self-regulation approach and aims to introduce more guarantees and protections for users, increasing autonomy and overcoming passivity with respect to the services offered, introducing measures to require greater transparency and accountability from companies, and introducing more obligations for platforms;

COMP 160 EPP (240), RE (241), Greens (238), ECR (239), Left (237)

AH. whereas the current *actions against disinformation campaigns on online* platforms are not *effective or deterrent* and *allow platforms to continue promoting discriminatory or malicious content;*

COMP 161 RE (247), Greens (248)

AL. whereas the lack of transparency with regard to the algorithmic choices of platforms makes it impossible to validate claims by platforms about what they do *and the effect of their action* to counter information manipulation and interference; *whereas there are discrepancies between the stated effect of their efforts in their annual self-assessments and their effectiveness as shown in the recent “Facebook Papers”;*

COMP 162 EPP (253), SD (249), RE (251), Greens (250), ECR (252)

AM. whereas *the non-transparent nature of targeted advertising leads to* massive amounts of online advertising *from* reputable brands, *sometimes even by public institutions, ending* up on websites *encouraging terrorism*, hosting hate speech and disinformation, *financing their growth*, without the *awareness* or consent of the advertisers;

COMP 163 SD (254, 257, 258, 790, 795, 797), RE (256), Greens (789)

AMa. whereas the online advertising market is controlled by a small number of big Ad Tech companies which divide the market amongst themselves with Google and Facebook are the biggest players; whereas this high market concentration on a few companies is associated with a strong power imbalance; whereas the use of clickbait techniques and the power of these few actors to determine which content gets monetized and which not, even though the algorithms they use cannot tell the difference between disinformation and normal news content constitutes a threat to diversified media; whereas the targeted advertising market is profoundly non-transparent; whereas Ad Tech companies force brands to take the hit for their negligence in monitoring where ads are placed;

Critical infrastructure and strategic sectors

COMP 164 EPP (263), RE (264)

AP. whereas the growing globalisation of the division of labour and of production chains has led to manufacturing and skills gaps in key sectors across the Union; whereas this has resulted in the EU's high import dependence on many essential products and primary assets, *which may incorporate built-in vulnerabilities*, coming from abroad; *whereas supply chain resilience ought to be among the priorities of EU decision-makers;*

COMP 165 EPP (265, 269, 818), SD (267, 273), RE (268), ID (266), Left (842)

AQ. whereas foreign direct investments (FDI) – investments by third countries *and foreign companies*– in strategic sectors in the EU, *but also in neighbourhood areas, such as the Western Balkans, in particular China's acquisition of critical structures*, have been a growing cause for concern in recent years, *considering the increasing importance of the trade-security nexus; whereas these investments pose a risk of creating economic dependencies and leading to a loss of knowledge in key production and industrial sectors;*

COMP 166 EPP (271), SD (274)

AQ a. whereas open strategic autonomy of the EU requires control of European strategic infrastructures; whereas the Commission and the Member States have expressed growing concern about security and control of technologies and infrastructure in Europe;

Foreign interference during electoral processes

COMP 167 SD (276, 277)

AQ d. whereas malicious actors that seek to interfere in electoral processes take advantage of the openness and pluralism of our societies as a strategic vulnerability to attack democratic processes and the resilience of the EU and its Member States; whereas it is in the context of electoral processes where foreign interference becomes more dangerous as citizens reengage and are more involved in conventional political participation;

COMP 168 SD (278, 280, 281)

AQ e. whereas the distinctive nature of foreign interferences in electoral processes, and the use of new technologies in this regard, as well as its potential effects, represent especially dangerous threats to democracy; whereas foreign interference in electoral processes goes well beyond social media “information warfare” favouring specific candidates to hack and target databases and gain access to information of registered voters, directly interfering with the normal functioning, competitiveness and legitimacy of the electoral process; whereas foreign interference actions aim to introduce doubts, uncertainty, mistrust and to delegitimize the entire electoral process and not only to modify the result of an election;

Covert funding of political activities by foreign actors and donors

COMP 169: EPP (282, 286), RE (283, 287, 288), ID (285), ECR (356, 380), Left (284)

AS. whereas, for instance, Russia, China and other authoritarian regimes, have funnelled more than USD 300 million into 33 countries to interfere in democratic processes, *as well as Iran and Venezuela or other-actors from the Middle-East and US far-right [which] have [also] been involved in covert funding*, and this trend is clearly accelerating; whereas half these cases concern Russia’s actions in Europe; *whereas corruption and illicit money laundering are one of the sources of political financing from authoritarian third countries;*

COMP 170: RE (255, 292, 295), ECR (293)

AT. whereas these operations *finance extremist, populist, anti-European parties and certain other parties and individuals* or movements aimed at deepening societal fragmentation and undermining the legitimacy of European and national public authorities; *whereas this has contributed to increase the reach of these parties or movements;*

COMP 170a: SD (296, 298, 299, 300, 301, 302, 303, 304, 378), RE (1046, 1047)

AT a. whereas Russia seeks out contacts to parties, figures and movements to use players within the European Institutions to legitimate Russian positions, Proxy-Governments, to lobby for sanctions relief and mitigate the consequences of international isolation; whereas parties like the Austrian FPÖ, the French Rassemblement National, the Italian Lega have signed a cooperation agreements with Russian President Vladimir Putin's United Russia party and are confronted with media reports about allegations on being willing to accept political party funding from Russia; whereas other European Parties like the German AfD, the Hungarian Fidesz and Jobbik and the Brexit Party in the UK are also reportedly having close contact with the Kremlin, and in case of the AfD and Jobbik also worked as so called 'election observers' in Kremlin-controlled elections, for example in Donetsk and Lugansk in eastern Ukraine, to monitor and legitimise Russian-sponsored elections; whereas findings about the close and regular contacts between Russian officials and representatives of a group of Catalan secessionists in Spain, as well as between the largest private donor for the Brexit vote.leave campaign, require an in-depth investigation, and are part of Russia’s wider strategy to use each and every opportunity to manipulate discourses in order to promote destabilisation;

COMP 171: EPP (307), SD (308), RE (306)

AU. whereas electoral laws, in particular provisions on the financing of political activities, are not ***coordinated enough*** at EU level, and therefore allow for opaque financing methods by foreign actors; ***whereas the legal definitions to of political donations are too narrowed, allowing foreign in-kind contributions to take place in the European Union;***

COMP 172: SD (309), RE (310)

AV. whereas, ***in some Member States***, online political advertising is not subject to the rules for offline political advertising; ***whereas there is a serious lack of transparency in online political advertising, which makes it impossible for regulators to enforce spending limits and prevent illegal sources of funding, with potentially disastrous consequences for the integrity of our electoral systems;***

Cybersecurity and resilience against cyberattacks

COMP 173 EPP (319), SD (318), Greens (320)

AX. whereas the incidence of cyberattacks ***and cyber-enabled incidents led by hostile state and non-state actors*** has been increasing in recent years; whereas several cyberattacks, such as the global spear-phishing email campaigns targeting strategic vaccine storage structures and the cyberattacks against the European Medicines Agency (EMA), ***European Banking Authority***, the Norwegian Parliament ***and countless others***, have been traced back to state-backed hacker groups, predominantly affiliated to the Russian and Chinese Governments;

COMP 174 SD (322), ECR (323)

AX a. ***whereas the European Union is committed to the application of existing international law in cyberspace, in particular the UN Charter; whereas malign foreign actors are exploiting the absence of a strong legal international framework in the cyber domain;***

COMP 175 EPP (955), SD (960, 961), RE (324, 968)

AY. ***whereas the Member States have increased their cooperation in the domain of cyber defence through the framework of PESCO, including through setting up Cyber Rapid Response Teams; whereas the European Defence Industrial Development Programme (EDIDP) included intelligence, secured communication and cyber-defence in its work programmes;*** whereas the current capacity to face cyber threats is limited owing to the scarcity of human and financial resources, ***for example in critical structures such as hospitals;*** ***whereas the EU has committed to invest 1.6 billion euros, under the Digital Europe programme,⁹ in the response capacity and deployment of cybersecurity tools for public administrations, businesses and individuals, as well as develop public-private cooperation;***

COMP 176 SD (327, 328, 395)

⁹ <https://www.consilium.europa.eu/en/policies/cybersecurity/>

AZ. whereas *gaps in and the fragmentation of the EU's capabilities* and strategies in the cyber field is becoming an increasing problem, *as pointed out by the European Court of Auditors¹⁰; whereas the EU Cyber Diplomacy Toolbox, set up in May 2019, has shown the added value of a joint EU diplomatic response to malicious cyber activities; whereas the Council decided for the first time on 30 July 2020 to impose restrictive measures against individuals, entities and bodies responsible for or involved in various cyber-attacks;*

COMP 177 SD (331), RE (329, 330), Greens (974)

BA. whereas massive-scale and illicit *use of* surveillance programs, *such as Pegasus*, have been used by foreign state actors to target journalists, human rights activists, *academics, government officials* and politicians, including European heads of state; *whereas Member States have also made use of the surveillance spyware;*

Protection of EU Member States, institutions, agencies, delegations and missions

COMP 178 SD (275, 335, 341), RE (334, 336, 342, 1008), Greens (343)

BB. whereas the decentralised and multinational character of EU institutions, *including its missions and operations, are an ever increasing target that is* exploited by malicious foreign actors wanting to sow division in the EU; *whereas there is an overall lack of security culture in EU institutions despite the fact that they are clear targets; whereas Parliament as the democratically-elected institution of the EU face specific challenges; whereas several cases revealed that EU institutions appear vulnerable to foreign penetration; whereas the safety of EU staff should be ensured;*

COMP 179 EPP (338), RE (337, 344)

BC. whereas it is necessary to have *strong and coherent* crisis management procedures in place *as a matter of priority; whereas additional training should be offered in order to enhance preparedness of staff;*

COMP 180 SD (345), RE (339, 340)

BD. whereas cyberattacks have recently targeted several EU institutions, which underlines the need for strong interinstitutional cooperation in terms of detecting, monitoring and sharing information during cyberattacks and/or with a view *of preventing them, including during EU CSDP missions and operations; whereas the EU and its Member States should organise regular, joint exercises to identify weak spots and take the necessary measures;*

Interference through global actors via elite capture, national diasporas, universities, and cultural events

COMP 181 EPP (349, 350), SD (351), Left (352)

BE. whereas a number of *politicians* former high-level European politicians and civil servants are hired or co-opted by foreign *authoritarian state-controlled national or*

¹⁰ https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

private companies, in exchange of their knowledge at the expense of the *interests of the citizens of the* EU and its Member States’;

COMP 182 SD (332, 355, 359), ECR (356)

BF. whereas *some* countries are particularly active in the field of elite capture and co-optation, *in particular* Russia *and* China, *but also Saudi Arabia and other Gulf countries*, with, for instance, former German Chancellor Gerhard Schröder and former Prime Minister of Finland Paavo Lipponen having both joined Gazprom to speed up the application process for Nord Stream 1 and 2, former Austrian Minister of Foreign Affairs Karin Kneissl appointed board member of Rosneft, former Prime Minister of France François Fillon appointed board member of Zaroubejneft, former Prime Minister of France Jean-Pierre Raffarin actively engaged in promoting Chinese interests in France, former Czech Commissioner Štefan Füle having worked for CEFC China Energy, *former Prime Minister of Finland Esko Aho now on the board of the Kremlin Sherbank, former French Minister in charge of Relations with the Parliament Jean-Marie Le Guen who is Member of the Board of Directors of Huawei Francek, or Yves Leterme, former Prime Minister of Belgium, Co-Chairman of the Chinese investment fund ToJoy, etc., and many other high level politicians and officials;*

COMP 183 SD (360, 361, 362, 363, 392)

BG. whereas economic lobbying strategies can be combined with foreign interference goals; *whereas according the OECD on “Lobbying in the 21st Century” only the US, Australia and Canada have rules in place that cover foreign influence; whereas there is a serious lack of legally binding rules and enforcement of the EU’s lobbying register, that makes it practically impossible to track lobbying coming outside of the EU; whereas there is currently no way of monitoring lobbying efforts in EU Member States who influence legislation and foreign policy through the European Council; whereas regulation regarding lobbying in the EU focuses mainly on face-to-face contact and does not take into account a whole existing ecosystem of different types of lobbying in Brussels; whereas countries like China and Russia, but also Qatar, the United Arab Emirates and Turkey have invested heavily in lobbying efforts in Brussels;*

COMP 184 SD (366), Greens (365)

BH. whereas *trying to instrumentalise vulnerable groups, including* the national *minorities and* diaspora living on EU soil represents an important element of foreign interference strategies;

COMP 185 EPP (369, 370), SD (358, 371), RE (372), ECR (368, 390)

BI. whereas different state actors, such as the Russian, Chinese, *and to a lesser degree the Turkish Government*, have been attempting to increase their influence *by setting up and* using cultural, educational (e.g. through grants and scholarships) and religious institutes *across EU Member States, in a strategic effort to destabilize European democracy and expand control over Eastern- and Central Europe; whereas the*

alleged difficult situation of its national minority has been used in the past by Russia as an excuse for direct intervention in third countries;

COMP 186 EPP (379), RE (375)

BJ. whereas there is evidence of Russian interference and online information manipulation in many liberal democracies around the world, including but not limited to the Brexit referendum in the United Kingdom, and the presidential elections in France and the US, and practical support of *extremist, populist, anti-European parties and certain other parties and individuals* across Europe, including but not limited to France, Germany, Italy and Austria; whereas *more support for research and education is needed to be able to understand what the exact influence of foreign interference was on specific events, such as the Brexit and the election of President Trump in 2016;*

COMP 187 EPP (172), RE (381, 382, 383, 384), ID (661)

BJ a. whereas Western based by the Russian state-controlled Sputnik and RT networks combined with Western media, fully or partially owned by Russian and Chinese legal and individual entities, actively engage into disinformation activities against liberal democracies; whereas Russia is resorting to historical revisionism, seeking to rewrite the history of Soviet crimes and promoting Soviet nostalgia among susceptible population in Central and Eastern Europe; whereas for national broadcasters in Central and Eastern Europe it is difficult to compete with Russian language TV content, funded by the Russian government; whereas there is a risk of an unbalanced cooperation between Chinese and foreign media, taking into account that Chinese media are the voice of the Chinese Communist Party at home and abroad;

COMP 188 SD (391), RE (386)

BK. whereas more than 500 Confucius centres have been opened around the world, including around 200 in Europe, and Confucius Institutes and Confucius Classrooms are used by China as a tool of interference within the EU; *whereas academic freedom is severely restricted in Confucius Institute; whereas universities or educational programs are the target of massive foreign funding notably from China or Qatar, such as the Fudan University in Budapest;*

Deterrence, attributions and collective countermeasures, including sanctions

COMP 189 EPP (398, 401), SD (397), RE (1108), Left (399)

BM. whereas the EU should strengthen its deterrence tools *and tools for attributing and categorising the nature of those attacks as violating or not violating international law, with a view to establishing an effective sanctions regime* so that malicious foreign actors have to pay the costs of their decisions and bear the consequences; *whereas targeting individuals might not be sufficient; whereas other tools, like trade measures, could be used to protect European democratic processes against state-sponsored hybrid attacks; whereas deterrence measures must be applied in a transparent process with all due guarantees; whereas hybrid attacks are calibrated*

so that they deliberately fall below Article 42(7) TEU and article 5 of NATO threshold;

Global cooperation and multilateralism

COMP 190 RE (1109), Greens (402), Left (403)

BN. *whereas malicious actions orchestrated by foreign **state and non-state actors** are affecting many democratic **partner** countries around the world; **whereas democratic allies depend on their ability to join forces in a collective response;***

COMP 191 EPP (417), SD (405, 406, 407, 408, 1145), RE (414), Greens (416)

*BN a. **whereas the European Accession countries in the Western Balkans are especially suffering under attacks through foreign interference and disinformation campaigns, stemming from both Russia, China and Turkey, such as for example Russia's interference campaigns that took place during the ratification process of the Prespa Agreement in North Macedonia; whereas the COVID-19 pandemic has been further exploited in the Western Balkans by China and Russia to destabilize the countries and discredit the EU; whereas candidate and potential candidate countries are expected to join the EU's initiatives in fighting foreign interference;***

COMP 192 EPP (409, 1158), SD (415)

BO. *whereas there is still a lack of common understanding and common definitions among like-minded partners **and allies** with regard to the nature of the threats at stake; **whereas the UN Secretary General is calling for a global code of conduct to promote integrity of public information; whereas the Conference on the Future of Europe is an important platform for discussions related to the topic;***

COMP 193 SD (419), RE (413), Greens (1194), ID (568), Left (412), 418

BP. *whereas there is a need for global, **multilateral** cooperation **and support** among like-minded partners in dealing with foreign malicious interference; **whereas other democracies have developed advanced skills and strategies, such as Australia or Taiwan; whereas Taiwan stands at the forefront of information manipulation, mainly from China; whereas the success of the Taiwanese system is founded on cooperation among all branches of government, but also with independent NGOs specialized in fact-checking and media literacy, as well as with social media platforms, such as Facebook, as well as the promotion of media literacy for all generations, the debunking of disinformation, and the curbing of the spread of manipulative messages; whereas the INGE committee had a three-day official mission to Taiwan to discuss disinformation and foreign electoral intervention;***

Citations

COMP 194 Greens (20), 19

- *having regard to the studies, briefings and in-depth analysis requested by the INGE Committee*

COMP 195 EPP (25), SD (24)

- having regard to the 2018 Code of Practice on Disinformation, to the 2021 Guidance on Strengthening the Code of Practice on Disinformation (COM(2021)0262), *and to the ERGA Recommendations for the New Code of Practice on Disinformation, October 2021,*