European Parliament
2019-2024

Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation

2020/2268(INI)

18.10.2021

DRAFT REPORT

on foreign interference in all democratic processes in the European Union, including disinformation
(2020/2268(INI))

Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation

Rapporteur: Sandra Kalniete

CONTENTS

Page

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

on foreign interference in all democratic processes in the European Union, including disinformation
(2020/2268(INI))

The European Parliament,

– having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7, 8, 11, 12, 39, 40, 47 and 52 thereof,

– having regard to the Convention for the Protection of Human Rights and Fundamental Freedoms, and in particular Articles 8, 9, 10, 11, 13, 16 and 17 thereof, and to the Protocol thereto, and in particular Article 3 thereof,

– having regard to the joint communications from the Commission and the High Representative of the Union for Foreign and Security Policy of 5 December 2018 entitled 'Action Plan against Disinformation' (JOIN(2018)0036) and of 14 June 2019 entitled 'Report on the implementation of the Action Plan Against Disinformation' (JOIN(2019)0012),

– having regard to the European democracy action plan (COM(2020)0790),

– having regard to the Digital Services Act package,

– having regard to the 2018 Code of Practice on Disinformation and to the 2021 Guidance on Strengthening the Code of Practice on Disinformation (COM(2021)0262),

– having regard to the European Court of Auditors' Special Report 09/2021 entitled 'Disinformation affecting the EU: tackled but not tamed',

– having regard to the Commission proposal of 16 December 2020 for a directive of the European Parliament and of the Council on the resilience of critical entities (COM(2020)0829) and to the proposed annex to the directive,

– having regard to Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union[1] (FDI Screening Regulation) and the March 2020 Guidance on the FDI Screening Regulation (C(2020)1981),

– having regard to the joint communication from the Commission and the High Representative of the Union for Foreign and Security Policy of 16 December 2020 on the EU's cybersecurity strategy for the digital decade (JOIN(2020)0018),

– having regard to the Commission proposal of 16 December 2020 for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020)0823),

[1] OJ L 79 I, 21.3.2019, p. 1.

– having regard to the March 2021 EU toolbox of risk mitigating measures on the cybersecurity of 5G networks,

– having regard to Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013[2],

– having regard to its decision of 18 June 2020 on setting up a special committee on foreign interference in all democratic processes in the European Union, including disinformation, and defining its responsibilities, numerical strength and term of office[3], adopted under Rule 207 of its Rules of Procedure,

– having regard to Rule 54 of its Rules of Procedure,

– having regard to the report of the Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (A9-0000/2021),

A. whereas foreign interference constitutes a serious violation of the universal values and principles on which the Union is founded, such as human dignity, freedom, equality, solidarity, respect for human rights and fundamental freedoms, democracy and the rule of law;

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 democratic processes in the EU and its Member States, such as the holding of free and fair elections;

C. whereas any action against foreign interference and information manipulation must itself respect the fundamental freedoms of expression and information;

D. whereas evidence shows that malicious foreign actors use information manipulation and other interference tactics to interfere in democratic processes in the EU; whereas these attacks mislead and deceive citizens, increase polarisation and divide society, worsen the situation of vulnerable groups, distort the integrity of democratic elections and referenda, and sow distrust in public authorities and democracy;

E. whereas foreign interference tactics take the form of disinformation and the suppression of information, but also the manipulation of social media platforms and advertising systems, cyberattacks, hack-and-leak operations, threats against and the harassment of journalists, researchers, politicians and members of civil society organisations, covert donations and loans to political parties, campaigns, organisations and media outlets, fake or proxy media outlets and organisations, elite capture and co-optation, fake personas, pressure to self-censor, the abusive exploitation of historical, religious and cultural narratives, pressure on educational and cultural institutions, taking control of

[2] OJ L 151, 7.6.2019, p. 15.
[3] Texts adopted, P9_TA(2020)0161.

critical infrastructure, pressuring foreign nationals living in the EU and espionage;

F. whereas foreign interference is a pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes; whereas such interference is manipulative in character, and conducted 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; whereas foreign actors' use of domestic proxies and cooperation with domestic allies blurs the line between foreign and domestic interference;

G. whereas there is a need to agree between like-minded partners on common definitions of foreign interference in order to establish international norms and standards;

Need for a coordinated EU strategy against foreign interference

H. whereas foreign interference attempts are increasing and becoming more sophisticated;

I. whereas it is the duty of the EU and its Member States to defend all citizens 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 and counter these threats;

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;

K. whereas the monitoring of the state of foreign interference in real time by institutional bodies and independent fact-checkers is crucial so that appropriate action is taken not only to provide information about ongoing malicious attacks but also to counter them;

L. whereas the resilience of EU citizens against foreign interference and information manipulation requires a long-term and whole-of-society approach;

M. whereas it is necessary to cooperate and coordinate across administrative levels and sectors to identify vulnerabilities, detect attacks and remedy them;

Building EU resilience through situational awareness, media literacy and education

N. whereas situational awareness is the first step towards countering information manipulation and interference;

O. whereas high-quality, sustainably-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; whereas professional media and traditional journalism, as a quality information source, are facing challenging times in the digital era; whereas, in spite of all the progress made in raising awareness of the situation, many people, including policy-makers and civil servants working in the areas potentially targeted, are still unaware of the risks linked to foreign interference and how to avoid them;

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;

Q. whereas there is a need to complement terminology that focuses on content, such as fake news and disinformation, with terminology that centres on behaviour, in order to adequately describe the problem;

R. whereas training in media and digital literacy and awareness-raising are important tools to make citizens more resilient against interference attempts in the information space;

S. whereas information manipulation can take many forms, such as spreading disinformation, distorting facts and representations of opinion, suppression of certain information or opinions, taking information out of context, promoting some opinions at the expenses of others, and harassing people to silence them;

T. whereas each section of society and each individual have important roles to play to stop the spread of disinformation and warn people in their environment who are at risk;

U. whereas it is important to have easy access to fact-based information when disinformation starts to spread;

V. whereas it is necessary to rapidly detect attempts to manipulate the information sphere in order to counter them;

W. whereas disinformation thrives 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;

X. whereas online platforms can be cheap and easy tools for those engaging in information manipulation and other interference, such as hate and harassment, silencing of opponents, espionage or spreading of disinformation;

Foreign interference using online platforms

Y. whereas we have witnessed ongoing 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 had very limited success in tackling them;

Z. whereas online platforms control the flow of information and advertising online, whereas platforms design and use algorithms to control these flows, and whereas platforms share very little or no information about the design, use and impacts of these algorithms;

AA. whereas numerous vendors registered in the EU sell fake likes, comments and shares to any actor wishing to artificially boost their visibility online; whereas it is almost impossible to identify legitimate uses of such services, while harmful uses include manipulating elections, promoting scams, negative reviews of competitors' products and defrauding advertisers;

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 is sold on the data market; whereas data leaks happen repeatedly; whereas such databases could be goldmines for malicious actors wanting to target groups or individuals;

AC. whereas opting not to share data is generally cumbersome and time-consuming in comparison with opting to share data;

AD. whereas online platforms are integrated into most parts of our lives and can have a huge impact on our thinking and behaviour, for instance when it comes to voting preferences or behaviour;

AE. whereas algorithm curation mechanisms, engineered to maximise engagement, are repeatedly reported to promote polarising and radicalising content;

AF. whereas the spread of the deepfake audio and video materials may become an ever-increasing problem;

AG. whereas self-regulation systems such as the 2018 Code of Practice on Disinformation have led to improvements, but leave too much room for platforms to do nothing or very little to combat interference in their systems;

AH. whereas the current sanctions that threaten those who use the platforms to abuse are not severe enough to deter them;

AI. whereas platforms dedicate significantly lower resources to content in lesser-spoken languages, and even for widely spoken non-English languages, compared to English content;

AJ. whereas platforms' action, or non-action, cannot be appealed by the organisation or individual affected;

AK. whereas in recent months, several major players have obeyed censorship rules, for example during the Russian parliamentary elections in September 2021, when Google and Apple removed Smart Voting apps from their stores in Russia;

AL. whereas the lack of transparency with regard to the algorithmic choices of platforms makes it next to impossible to validate claims by platforms about what they do to counter information manipulation and interference;

AM. whereas massive amounts of online advertising by reputable brands ends up on websites hosting hate speech and disinformation, without the knowledge or consent of the advertisers;

Critical infrastructure and strategic sectors

AN. whereas the management of threats to critical infrastructures, especially when part of a synchronised, malicious hybrid strategy, requires coordinated, joint efforts across sectors, at different levels – EU, national, regional and local – and at various times;

AO. whereas the Commission has proposed a new directive to enhance the resilience of

critical entities providing essential services in the EU, which includes a proposed list of new types of critical infrastructure; whereas the list of the services will be set out in the annex to the directive;

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 coming from abroad;

AQ. whereas foreign direct investments (FDI) – investments by third countries – in strategic sectors in the EU have been a growing cause for concern in recent years;

Covert funding of political activities by foreign donors

AR. whereas solid body of evidence shows that foreign actors have been actively interfering in the democratic functioning of the EU and its Member States, particularly during election and referendum periods, through covert funding operations;

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, and this trend is clearly accelerating; whereas half these cases concern Russia's actions in Europe;

AT. whereas these operations are aimed at financing European political parties or movements aimed at deepening societal fragmentation and undermining the legitimacy of European and national public authorities;

AU. whereas electoral laws, in particular provisions on the financing of political activities, are not harmonised at EU level, and therefore allow for opaque financing methods by foreign actors, through various rules creating many loopholes and legal or illegal practices within the EU;

AV. whereas online political advertising is not subject to the rules for offline political advertising;

AW. whereas Regulation (EU, Euratom) No 1141/2014 of 22 October 2014 on the statute and funding of European political parties and European political foundations[4] is being revised with a view to achieving a greater level of transparency in terms of the financing of political activities;

Cybersecurity and resilience against cyberattacks

AX. whereas the incidence of cyberattacks 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) and the Norwegian Parliament, have been traced back to state-backed hacker groups, predominantly affiliated to the Russian and Chinese Governments;

AY. whereas the current capacity to face cyber threats is limited owing to the scarcity of

[4] OJ L 317, 4.11.2014, p. 1.

human and financial resources;

AZ. whereas the Union's fragmented capabilities and strategies in the cyber field is becoming an increasing problem;

BA. whereas massive-scale and illicit surveillance programs have been used by foreign state actors to target journalists, human rights activists, and politicians, including European heads of state;

Protection of EU institutions

BB. whereas the decentralised and multinational character of EU institutions can be exploited by malicious foreign actors wanting to sow division in the EU;

BC. whereas it is necessary to have proper crisis management procedures in place before the crises happen;

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 to their prevention;

Interference through elite capture, national diasporas and universities

BE. whereas a number of former high-level European politicians and civil servants are hired or co-opted by foreign companies controlled by States operating malicious interference within the EU, in exchange of their knowledge at the expense of the EU and its Member States' interests;

BF. whereas two countries are particularly active in the field of elite capture and co-optation, namely Russia and China, 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, and former Czech Commissioner Štefan Füle having worked for CEFC China Energy;

BG. whereas economic lobbying strategies can be combined with foreign interference goals;

BH. whereas controlling the national diaspora living on EU soil represents an important element of foreign interference strategies;

BI. whereas different state actors, such as the Russian Government and the Chinese Communist Party, have been attempting to increase their influence using cultural, educational (e.g. through grants and scholarships) and religious institutes;

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 for far-right and other radical-minded forces and actors across

Europe, including but not limited to France, Germany, Italy and Austria; whereas recent findings about the close and regular contacts between Russian officials and representatives of a group of Catalan secessionists in Spain require an in-depth investigation, given the constant attempts by Russia to exploit any matter it can to promote internal destabilisation and disunity in the EU;

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;

Deterrence and collective sanctions

BL. whereas the EU and its Member States do not currently have a specific regime of sanctions related to foreign interference and disinformation campaigns orchestrated by foreign state actors, meaning that these actors can safely assume that their destabilisation campaigns against the EU will meet with no consequences;

BM. whereas the EU should strengthen its deterrence tools so that malicious foreign actors have to pay the costs of their decisions and bear the consequences;

Global cooperation and multilateralism

BN. whereas malicious actions orchestrated by foreign authoritarian regimes are affecting many different democratic countries around the world;

BO. whereas there is still a lack of common understanding and common definitions among like-minded partners with regard to the nature of the threats at stake;

BP. whereas there is a need for global cooperation among like-minded partners in dealing with foreign malicious interference;

Need for an EU coordinated strategy against foreign interference

1. Is deeply concerned about the growing incidence and increasingly sophisticated nature of foreign interference and information manipulation attempts targeting all parts of the democratic functioning of the European Union and its Member States;

2. Calls on the Commission to propose, and the co-legislators and Member States to support, a multi-layer and cross-sector strategy, as well as adequate financial resources, aimed at equipping the EU and its Member States with appropriate resilience policies and deterrence tools, enabling them to tackle all hybrid threats and attacks orchestrated by foreign countries; considers that this strategy should be built on: 1 – common definitions, critical and ex post impact assessment of the legislation adopted so far, as well as understanding and situational awareness of the issues at stake, 2 – concrete policies enabling resilience-building among EU citizens in line with democratic values, 3 – appropriate disruption capabilities, and 4 – diplomatic and deterrence responses in a global context;

3. Underlines that all measures to prevent, detect and counter foreign interference must be designed in way that respects and promotes fundamental rights, including respect for private life and the freedoms of thought, expression and information;

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 literacy and education,

   b) foreign interference using online platforms,

   c) critical infrastructure and strategic sectors,

   d) covert funding of political activities by foreign donors,

   e) cybersecurity and resilience against cyberattacks,

   f) protection of EU institutions,

   g) interference through elite capture, national diasporas and universities,

   h) deterrence and collective sanctions,

   i) global cooperation and multilateralism;

5. Calls, in particular, for the EU to increase the resources and means allocated to bodies and organisations tasked with monitoring and raising awareness of the severity of threats including disinformation, to strengthen the protection of the strategic interests and infrastructure of the EU and its Member States, and to build international cooperation with like-minded partners facing similar challenges;

6. Is concerned about the overwhelming lack of awareness of the severity of the current threats posed by foreign authoritarian regimes targeting all levels and sectors of European society, aimed at undermining public authorities' legitimacy, and deepening political and social fragmentation;

7. Is concerned about the lack of appropriate and sufficient measures to prevent, detect and counter these interference attempts, making interference an attractive tactic for malicious actors since the risks of being sanctioned, or even noticed, are very low;

8. Urges the Commission to include a foreign information manipulation and interference perspective in the ex ante impact assessment carried out before presenting new proposals; suggests that the Commission also perform regular resilience reviews in which it assesses the development of the threats and their impact on current legislation and policies;

9. Calls on the Commission to analyse recent national setups, 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, and France's new national agency Viginum, to see which best practices could be implemented at EU level;

10. Is concerned about the many gaps and loopholes in current legislation and policies at EU and national level intended to detect, prevent and counter interference;

11. Calls on the Commission to set up an EU mechanism dedicated to scrutinising existing legislation and policies to identify gaps that could be exploited by malicious actors and swiftly suggest ways 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;

12. 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;

Building EU resilience through situational awareness, media literacy and education

13. Stresses that EU institutions and Member States need sound and robust 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;

14. Underlines that it is equally important that the insights from this analysis do not stay within groups of foreign interference specialists, but are shared with the broader public, especially with people performing sensitive functions, so that everyone is aware of the threat patterns and can avoid the risks;

15. Underlines that it is necessary to develop a common methodology for developing situational awareness, collecting systematic evidence and detecting manipulation of the information environment, as well as standards for technical attribution;

16. Stresses the need for the EU, in cooperation with Member States and global partners, to develop a conceptual definition of the interference threat; underlines that this definition needs to reflect the tactics, techniques and procedures that describe the patterns of behaviour of the threat actors that we see today;

17. Calls for the EU institutions to further develop 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 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;

18. Underlines the need to strengthen monitoring efforts well ahead of elections or other important political processes;

19. Calls on Member States to make full use of these resources by sharing relevant intelligence and actively participating in the Rapid Alert System; is of the opinion that analysis and intelligence cooperation needs to be strengthened even more;

20. Welcomes Commission President von der Leyen's idea of establishing a Joint Situational Awareness Centre, while expecting further clarification of its set-up and

mission; underlines that such a centre would require active cooperation with the services of the Commission, the EEAS, the Council and Parliament;

21. Recalls the need to equip the EEAS with a mandate and the necessary resources to monitor and address information manipulation and interference beyond the regions currently covered by the three taskforces, 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; stresses further the need to significantly boost expertise and language capacity with regard to China and other strategically important regions, both in the EEAS and the EU institutions in general;

22. Stresses the importance of independent journalists, fact-checkers and researchers for 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;

23. Praises the indispensable research and the many creative and successful media and digital literacy and awareness-raising initiatives carried out by individuals, schools, universities, media organisations, public institutions and civil society organisations;

24. Calls for reliable and sustainable public funding sources for independent fact-checkers, researchers, quality media and journalists, and NGOs investigating information manipulation and interference, promoting media literacy and other means to empower citizens, and researching how to meaningfully measure the effectiveness of media literacy training, awareness-raising, debunking and strategic communication; underlines that several countries around the globe are taking steps to ensure that the media have adequate financial resources; welcomes, in this regard, the new funding possibilities for media literacy in the 2021-2027 Creative Europe programme;

25. Underlines the need to make analysis, incident reports and intelligence with regard to information manipulation and interference available to the public; therefore suggests the creation of a public repository, with key information available in all EU languages;

26. Calls on all Member States to include media and digital literacy, as well as critical thinking and public participation, in their curricula, from early years to adult education, including training for teachers and researchers;

27. Calls for the EU institutions and Member States, at all administrative levels, to identify sectors at risk of interference attempts and provide regular training and exercises for staff working in these sectors in how to detect and avoid interference attempts, and underlines that such efforts would benefit from a standardised format established by the EU; recommends that introductory training also be offered to all public servants; welcomes in this regard the training offered to Members and staff by Parliament's administration; recommends that this training be developed further;

28. Underlines the need to raise awareness about the phenomenon of information manipulation and 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 and visitors, both offline and

online, in Brussels and other EU capitals, and recommends that they be further developed;

29. Calls on the Member States, the EU administration and civil society organisations to share best practices for media 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;

30. Calls for the EU and its Member States to implement targeted awareness-raising and media literacy programmes aimed at 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;

31. Calls on the Commission to put forward a media literacy strategy with a special focus on combating information manipulation;

32. Underlines the importance of strategic communication to counter the most common anti-democracy narratives; stresses that all democratic organisations need to defend democracy and have a common responsibility to engage with citizens, using their preferred languages and platforms;

33. Is concerned about the spread of foreign state propaganda, originating in Moscow and Beijing, which is translated into local languages, for instance in RT-, Sputnik- or Chinese Communist Party-sponsored media content disguised as journalism, and distributed with newspapers; is concerned about how these narratives have spread into real journalistic products;

34. Is deeply concerned about harassment and threats against journalists and calls on the Commission to swiftly submit concrete and ambitious proposals on the safety of journalists and media professionals, as announced under the European Democracy Action Plan;

35. Stresses the need to involve local and regional decision-makers responsible for strategic decisions in the areas that fall under their competence, such as infrastructure, cybersecurity, culture and education; underlines that local and regional politicians and authorities can often identify concerning developments at an early stage and stresses that local knowledge is often needed to identify and implement adequate countermeasures;

36. Recommends that Member States establish communication channels that companies, NGOs and individuals can turn to if they fall victim to information manipulation or interference; calls on the Member States to support those who are victims of attacks or are being put under pressure;

Foreign interference using online platforms

37. Stresses that freedom of expression must not be misinterpreted as freedom to engage in online activities that are illegal offline, such as harassment, espionage and threats; underlines that platforms need not only to abide by the law, but also to live up to the terms and conditions they promise their users;

38. Underlines the need, above all, for significantly increased transparency as regards the operations conducted by online platforms;

39. Calls for regulation to oblige platforms to do their part to reduce information manipulation and interference, for instance by using labels that indicate the true authors behind accounts, containing accounts regularly used to spread disinformation or that regularly break the terms and conditions of the platform, suspending inauthentic accounts used for coordinated interference campaigns or demonetising disinformation-spreading sites;

40. 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; recommends that the final reading of these texts take into account the aspects set out in the remainder of this section;

41. Calls for binding EU rules to limit 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, to decouple the different functions of platforms in order to reduce the amount of information available about each individual, and to make it equally easy to disagree as to agree to the storage and sharing of data; calls for an EU ban on micro-targeting for political or issue-based advertisement;

42. Calls for binding EU rules to require platforms to regularly identify, assess and mitigate risks of information manipulation and interference that using their services carries, to oblige platforms to set up systems to monitor how their services are used, in at least all official national and regional languages, 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;

43. Calls for the regulation of services offering social media manipulation tools and services; underlines that this regulation needs to be based on a thorough assessment of current practices and the associated risks;

44. Stresses the general need for transparency as regards the real natural or legal person behind online content and accounts; calls on platforms to introduce mechanisms to detect and suspend fake accounts linked to coordinated influence operations; underlines that demands for proof must allow for anonymity for persons in vulnerable positions (e.g. whistle-blowers or dissidents and political opponents of autocratic regimes) and allow room for satirical and humorous accounts;

45. Underlines that a greater responsibility to remove illegal and dangerous content must not lead to the arbitrary removal of legal content; urges caution as regards entirely suspending the accounts of real individuals;

46. Calls for binding rules to require platforms to create easily available communication channels for people or organisations who want to report abuse or suspected interference or manipulation, and to put in place appeal procedures, both for victims of content posted online 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;

47. Calls for rules to make online proceedings transparent, such as obligating platforms to set up public and easily searchable archives of online advertisements and give meaningful access to information about the design, use and impact of algorithms and individual-level data to vetted researchers affiliated with academic institutions, journalists, civil society organisations and international organisations representing the public interest;

48. Calls on platforms to correct the balance between the business-driven need to encourage people to stay on platforms longer by feeding them engaging content and the responsibility to promote quality content; urges platforms to ensure that their algorithms do not promote illegal, extremist or radicalising content, but rather offer users a plurality of perspectives;

49. Calls for algorithms to be modified in order to dismantle content originating from inauthentic accounts and channels that artificially drive the spread of harmful foreign information manipulation;

50. Stresses the need for a systematic review of the consequences of algorithms; underlines that such a review should also examine whether platforms can meet the guarantees promised in their respective terms and conditions and whether they allow large-scale, coordinated inauthentic behaviours to manipulate the content shown on their platforms;

51. Is alarmed by the massive number of online advertisements by reputable brands that end up on, and therefore finance, malicious websites promoting hate speech and disinformation, without the consent or even knowledge of the brands concerned; considers that programmatic advertising services, such as Google Ads and other ad exchanges, should be responsible for selecting publishers' websites listed in their inventory in order 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;

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 and assessment 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;

Critical infrastructure and strategic sectors

53. Considers that, given its interconnected and cross-border nature, critical infrastructure is increasingly vulnerable to outside manipulation 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;

54. Recommends that when considering the above proposal, efforts be made to strengthen the already well-coordinated connection and communication channels used by multiple actors, support to the competent authorities in Member States through the Critical

Entities Resilience Group, and the exchange of best practices not only among Member States but also, at regional and local level, 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;

55. Is of the opinion that the list of critical infrastructure could be extended to include the media, as well as election infrastructure, given their crucial importance in guaranteeing the functioning 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;

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;

57. Recommends taking a highly adaptable approach allowing for fast updates and modifications of the proposed directive, based on assessments of the threats, risks and vulnerabilities conducted by the Joint Research Centre in conjunction with the EEAS's INTCEN; underlines the need to design a modular method to ensure rapid adaptability and flexibility;

58. Believes that the EU and its Member States need to provide financing alternatives to prevent large parts of their critical infrastructure from coming into the possession of third countries, 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 in critical structures, and calls for a stronger regulatory framework to ensure that more competences in screening FDIs are transferred to EU institutions; believes that the framework should be better connected with independent analyses, either by national and EU institutes or by relevant think tanks; considers that it might also be appropriate to include other strategic sectors in the framework, such as 5G, so as to limit its dependency on high-risk suppliers;

59. Believes that the EU faces more challenges as a result of its dependence on foreign suppliers of technology; believes that the EU's move towards greater strategic autonomy and digital sovereignty is very important and the right way forward; considers the European Chips Act announced by the Commission, to ensure that parts that are vital for the production of chips are manufactured in Europe, 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 so as to 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;

60. Welcomes the European Union's development of GAIA-X, a European network of data infrastructure and service providers with European security standards, as an important step in resisting the dominance of US cloud service providers;

61. Calls on the Commission to propose actions to build a secure and sustainable supply of the raw materials used to produce batteries and renewable energy equipment;

Covert funding of political activities by foreign donors

62. 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 the EU to engage in any covert activity financed by a foreign power that aims to influence the process of European politics;

63. Points out that a substantial proportion of covert funding by foreign actors is not strictly speaking illegal because it is allowed by the numerous loopholes resulting from different provisions related to the financing of political activities in the Member States' national election laws;

64. Points out that these loopholes include:

a) in-kind contributions from foreign actors to political parties, including financial loans from any legal or physical persons based abroad, which should be prohibited;

b) straw donors with domestic citizenship[5]: transparency on physical and legal donors must be enforced through conformability statements attesting to the status of the donor, and greater enforcement powers given to electoral commissions;

c) shell companies and domestic subsidiaries of foreign parent companies[6]: shell companies should be prohibited and more robust requirements established in order to reveal the origins of funding through parent companies;

d) non-profit organisations and third parties[7], 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;

e) online political advertisements, which are not subject to the rules on TV, radio and print advertising and are usually not regulated at all: there is therefore a need to guarantee complete transparency with regard to the inflow and outflow of the money involved in online political advertisements, as well as to ensure much greater accountability as to the use of algorithms in line with the 'know your customer' principle; the Commission should swiftly submit a legislative proposal on the transparency of sponsored political content, as proposed under the European Democracy Action Plan, which will guarantee the effective right of EU parties to campaign online ahead of the European elections;

65. Calls on the Commission, therefore, to submit concrete proposals aimed at closing all

[5] Person who donates someone else's money to a political party or candidate using their own name.
[6] 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.
[7] 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.

loopholes allowing for the opaque financing of political parties 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 a ban on donations to political parties from outside the EU and the European Economic Area (EEA), with the exception of voters living outside the EU and the EEA;

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;

Cybersecurity and resilience against cyberattacks

67. Urges the EU institutions to rapidly increase investments in the Union's strategic digital capacities and capabilities, such as artificial intelligence, secured communication, and data and cloud infrastructure, in order to improve the Union's cybersecurity; calls on the Commission to also invest more in increasing the Union's digital knowledge and technical expertise so as to better understand the digital systems used across the Union; calls on the Commission to allocate additional resources, both human and financial, to the cybersecurity of both the EU institutions and the Member States;

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[8] (NIS2); 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, introducing stricter enforcement requirements, such as harmonised sanctions, and suggesting horizontal regulations and good public-private cooperation at operational level; 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;

69. Calls on the Commission to develop the EU toolbox of risk-mitigating measures for the new generation of technologies, such as 5G and 6G, so as to better take into account risks linked to the use of software and hardware produced by companies under the control of foreign authoritarian states, and to develop global standards and competition rules, in accordance with democratic values, for this new technology; 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;

70. Supports the Commission's idea of creating a Cyber Resilience Act that would complement a European Cyber Defence Policy, as cyber and defence are interconnected; calls for more resources for European cyber defence capabilities and coordination;

71. Condemns the massive and illicit use of the Pegasus surveillance software by state

[8] Proposal for a directive of the European Parliament and of the Council on measures for a high level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020)0823).

entities against journalists, human rights defenders and politicians; recalls that Pegasus is only one of the many examples of illicit surveillance programs run by state entities against innocent citizens;

72. Is worried that journalists and democracy activists can be illegally kept under surveillance and harassed by the authoritarian regimes they sought to escape, even on EU soil, and considers that this represents a grave violation of the fundamental values of the Union and of the fundamental rights of individuals, as provided for in the Charter of Fundamental Rights, the European Convention on Human Rights (ECHR) and the International Covenant on Civil and Political Rights; regrets the lack of legal support provided to the victims of this spy software;

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;

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 General Data Protection Regulation and the Data Protection Law Enforcement Directive; 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; 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 institutions

75. Underlines that the EU institutions' networks, buildings and staff represent a target for all types of hybrid threats and attacks by foreign state actors and should, therefore, be properly protected; 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;

76. Calls for a thorough review of the services, networks, equipment and hardware of the EU institutions, bodies and agencies used to ensure cybersecurity; 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;

77. Stresses the importance of 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; appreciates the recent initiatives taken by the Secretaries-General of the EU

institutions to develop common information and cybersecurity rules;

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-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;

79. Looks forward to the European Court of Auditors' Cybersecurity Audit Special Report, expected in early 2022;

80. Calls on all the EU institutions to raise awareness among their staff through proper training and guidance in order to mitigate and address cyber, and non-cyber, security risks; calls for mandatory and regular security training for all staff and MEPs;

81. Stresses the need for proper crisis management procedures for information manipulation cases, including alert systems between administrative levels and sectors, in order to ensure the provision of mutual information and prevent information manipulation from spreading; welcomes, in this regard, the Rapid Alert System (RAS) and rapid alert procedure established prior to the 2019 European elections and the procedures in place in the Commission and Parliament administrations to warn of possible cases affecting the institutions or EU democratic processes; asks the EU administration to reflect further on a shared toolbox to be activated in the event of an RAS alert;

Interference through elite capture, national diasporas and universities

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 be strictly prohibited;

83. Calls on the Commission to encourage and coordinate actions against elite capture, such as complementing the cooling-off periods for EU Commissioners with a reporting duty after the period, and structured rules to tackle elite capture at EU level;

84. Is concerned about integrated lobbying strategies combining industrial interests and foreign political goals, in particular when they favour the interests of an authoritarian state; calls, therefore, for the EU institutions to reform the Transparency Register, including by introducing more stringent transparency rules, mapping foreign funding for EU-related lobbying, and ensuring an entry which allows for the identification of funding from foreign governments; considers Australia's Foreign Influence Transparency Scheme to be a good practice to follow;

85. Calls on the Member States to consider the establishment of a foreign influence registration scheme and the creation of a government-managed register of declared activities undertaken for, or on behalf of, a foreign state, following the good practice of other like-minded democracies;

86. Is concerned by the attempts to control the diasporas living on EU soil by foreign authoritarian states; points out the crucial role played by China's United Front, which is a department reporting directly to the Central Committee of the Chinese Communist Party and tasked with coordinating the external interference strategy of China through the strict control of Chinese individuals and Chinese companies abroad; points out the experiences of Australia and New Zealand in dealing with the United Front;

87. Underlines that the efforts of the Kremlin to implement 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;

88. Is alarmed by the extraterritorial application of coercive measures stemming from China's new National Security Law, 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;

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; regrets, in particular, the decision taken by the museum of Nantes to cancel the exhibition on Genghis Kahn in 2020, following strong pressure from China opposing such an exhibition[9];

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 calls on the Commission and Member States to ensure proper budgetary allocations for European universities; calls on the Commission to propose legislation on increasing the transparency of the financing of universities, such as through mandatory donation declarations;

91. Is concerned about the increasing number of Confucius Institutes established around the world, and in particular in Europe, which are closely linked to the Chinese state; remarks that the Confucius Institutes changed their name in 2020 and are now known as the 'Center for Language Education and Cooperation'; points out the Confucius Institutes' lack of legal status; calls on Member States and the Commission to support independent Chinese language courses without the involvement of the Chinese Communist Party and the Chinese state; believes that the recently established National China Centre in Sweden could serve as an important asset in giving context to the actions and communications of the Confucius Institutes;

92. Considers, in addition, that Confucius Institutes serve as a lobbying platform for Chinese economic interests and for the Chinese intelligence service and the recruitment of spies; recalls that many universities have decided to terminate their cooperation with

[9] https://www.chateaunantes.fr/expositions/fils-du-ciel-et-des-steppes/

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;

93. Observes that foreign interference can also be pursued through influence in religious institutes, such as Russian influence in Orthodox churches, in particular in Serbia and Montenegro, including sowing division among local populations, developing a biased writing of history and promoting an anti-EU agenda, and Turkish influence through mosques in France and Germany; calls on the Commission and Member States to ensure better coordination on protecting religious institutes from foreign interference;

Deterrence and collective sanctions

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 States[10] and the EU Global Human Rights Sanctions Regime[11], adopted on 17 May 2019 and 7 December 2020 respectively, have demonstrated added value in providing the EU with valuable deterrence tools; recalls that the cyberattack and human rights sanctions regimes have been used twice, in 2020 and 2021 respectively;

95. Calls for the EU and its Member States to, take further measures against disinformation and hybrid threats, with full respect for the freedoms of expression and of information, including in the form of setting up a sanctions regime 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) in the field of foreign interference, including disinformation, which should target as far as possible the decision-makers and bodies responsible for aggressive actions; 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;

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;

97. Considers that while the nature of these hybrid attacks varies, their danger to the European Union's 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, may be substantial in terms of either the scale of the attacks, their nature or their cumulative effect; believes that a deeper analysis of the nature and impacts of individual disinformation and hybrid threats and actions that do not fall under the above-mentioned sanctions regime already in place for cyberattacks needs to be performed in order to categorise the attacks and define those that do not merit an EU response;

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2019%3A129I%3ATOC
[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2020:410I:TOC

98. Points out that the understanding that certain foreign interference actions are seriously affecting democratic processes and influencing the exercise of rights or duties is gaining ground internationally; points out, in this regard, the amendments adopted in 2018 in the Australian National Security Legislation Amendment (Espionage and Foreign Interference) Act, which aims to criminalise covert and deceptive activities by foreign actors intending to interfere with political or governmental processes, impact rights or duties, or support the intelligence activities of a foreign government, by creating new offences such as 'intentional foreign interference';

99. Is aware that pursuant to Article 21(3) TEU the Union must ensure consistency among the different areas of its external action and among these and other policies, as defined in the Treaties; points out, in this respect, that foreign interference, such as the threat posed by foreign terrorist fighters and groups who influence individuals remaining in the EU, was also tackled through Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism[12];

100. Underlines that, in order to reinforce their impact, sanctions should be imposed collectively based 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; refers, in particular, to 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 attack[13];

Global cooperation and multilateralism

101. Acknowledges that many democratic countries over the world are facing similar destabilisation operations carried out by foreign authoritarian states;

102. Highlights the need for global cooperation between like-minded countries 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;

103. Considers that, on the basis of common situational awareness, like-minded partners should exchange best practices and identify common responses, including collective sanctions;

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;

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;

[12] OJ L 88, 31.3.2017, p. 6.
[13] https://www.nato.int/cps/en/natohq/news_185000.htm

106. Welcomes the initiatives already taken, in particular at administrative level, to share knowledge about the state of hybrid attacks, including disinformation operations, in real-time, such as the EEAS-established Rapid Alert System partly opened to like-minded third countries, the G7-established Rapid Response Mechanism, and the NATO Joint Intelligence and Security Division;

107. Underlines that global cooperation should be based on common projects, involving international organisations such as the Organisation for Economic Co-operation and Development and UNESCO, and setting up democratic capacity-building in countries facing similar foreign hybrid threats; calls for the EU to establish a European Democratic Media Fund to support independent journalism in European neighbourhood countries;

108. Stresses the importance of strategic countries such as those in the Eastern and Southern Neighbourhoods of the EU and the Western Balkans, since Russia is trying to use these countries as an information manipulation and hybrid warfare laboratory; considers that EU actions can take the form of financing projects aimed at ensuring media freedom and cooperation on media literacy; draws attention to the need to strengthen EEAS capacity in this regard;

109. Calls for Parliament 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;

110. Calls for the EEAS to strengthen the role of the EU delegations in third countries in order to reinforce their ability to debunk disinformation campaigns threatening democratic values orchestrated by foreign state actors;

111. Calls for the issue of foreign malicious interference to be addressed within the upcoming new Strategic Compass of the EU;

°

° °

112. Instructs its President to forward this resolution to the Council, the Commission, the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy, and the governments and parliaments of the Member States.

EXPLANATORY STATEMENT

Background

When the European Parliament decided on 18 June 2020 to set up a Special Committee on Foreign Interference, including Disinformation, it tasked it with the mandate to provide a long-term approach to addressing evidence of foreign interference in the democratic institutions and processes of the EU and its Member States.

One year after the constitutive meeting of the committee on 23 September 2020, and based on a long series of testimonies from various experts and practitioners, the rapporteur can already lay out the reality, the extend of the scope and the extreme sophistication of the myriad of forms taken by the aggressive interference operations decided and funded by foreign actors against the EU; the rapporteur can also point out, with concerns, the rapidity of the adaptation, the volatility and the acceleration of this phenomenon - through new actors, new narratives, new tools within a period of just one year.

From the new-scale disinformation campaigns related to COVID-19 to the cyber-attacks against public authorities entities including public health infrastructures, from the interference strategies integrating elite capture and industrial lobbying to the covert financing of political activities, from the control of academic and cultural centres to the instrumentalisation of national diasporas, our committee has been analysing the multi-faceted and dynamic dimension of this new type of warfare whose purpose is to undermine the social cohesion and mutual trust of our European democratic societies in order to weaken them.

The committee has fortunately also witnessed the raise of the awareness about these crucial issues, including the commonly shared understanding that the EU and its Member States should swiftly be equipped with fully-fledged resilience policies and deterrence tools, based on a whole-of-society approach, enabling them to tackle all types of hybrid threats and attacks and, therefore, protecting the sustainable functioning of democracy.

Building EU resilience through situational awareness, media literacy and education

It is clear that the first basis for a strong defence against foreign interference is to have situational awareness. To gain this, we have two important steps: first, we need to monitor, map and analyse the difference interference attacks so we fully understand the threat; secondly, we need to make sure that everybody who needs to know is aware of this analysis.

There are plenty of researchers, civil society organisations, journalists and staff members of national or European institutions who do an excellent job in investigating the threat. We have met many of them in INGE. At the European level, the rapporteur especially appreciates the work of the EEAS StratCom taskforces. However, we need to develop this further. We cannot accept that there is still no taskforce monitoring interference coming from China.

We also need to make sure that the insights are spread to a wider audience. Both targeted trainings for people with functions sensitive to foreign interference and general awareness-raising campaigns are important. In this context, media and digital literacy education is crucial to empower citizens to better interpret and evaluate the information they encounter.

Journalists play a crucial role in ensuring a healthy debate climate. Unfortunately, they have

suffered financially of the digitalisation, especially when the advertisement systems seem to give advantage to emotional content, including opinions and disinformation, over quality journalism. Individual journalists are also often victims of harassments and organised threats when they cover sensitive topics. Whereas it is important to defend the independence of quality media, it is also important to investigate ways to support news outlets and journalists, both financially and against harassment.

Foreign interference using online platforms

It is clear that the current system of information spreading via platforms leads to a twisted online climate in which disinformation and other kinds of information manipulation thrive. The reports about leaks and selling of sensitive data, algorithms promoting radicalising content and platforms turning the blind eye to clear breaches of the law or of their own terms and conditions are so common that we almost get used to it and stop getting upset. We need to stop this.

Discussion after discussion with experts have convinced me that the current self-regulatory method do not work and needs to be replaced with binding rules. We cannot accept that foreign actors can freely manipulate the content we receive online via platforms or misuse advertisement systems so that advertisers unintentionally help fund them. We also cannot accept that the platforms are allowed to do nothing without consequences.

Admittedly, there have been many improvements, both on the initiative of the platforms themselves and originating in public measures like the Code of Practice. However, without meaningful transparency, it is impossible to make oneself a picture of the impact of these actions. It is also essential that The Code of Practice, which is voluntary by nature, has an effective enforcement mechanism and is complemented by a strong legislation. In addition, it is striking how many anti-interference policies are only used for English language content or content in a very limited number of languages. We cannot accept a situation where Latvian, Bulgarian, Greek or even French or German-speaking get much less protection against online manipulation than English native speakers just because the platforms prioritise English content.

Critical infrastructures and strategic sectors

Critical infrastructures are essential to the functioning of the economy and of society. To better protect critical sectors, there is a need for coordinated and joint efforts across all sectors and at different levels - EU, national, regional and local. The new Commission Directive to enhance the resilience of critical entities is an important starting point. However, the rapporteur believes the list of critical infrastructures should be enlarged to media as well as election infrastructures given their respective crucial importance in guaranteeing functioning of the EU and its Member States, and that flexibility should be allowed in the addition of new strategic sectors in the future. It is of the upmost importance that the Directive maintains a highly adaptable approach allowing for fast updates and modifications.

In addition, the dependence of both foreign investments and foreign suppliers of technology in critical infrastructures creates many threats to the autonomous functioning of these infrastructures. The EU's push towards strategic autonomy and digital sovereignty is therefore pivotal in countering these threats.

Covert funding of political activities by foreign donors

Solid evidence show that foreign actors have been actively interfering in the democratic elections and referendum of the European countries, through covert funding operations during the campaigns.

These malicious operations put at risk the integrity of the elections organised in the EU, since they bring unfair competition between parties and candidates in allocating further resources to some of the parties – usually the anti-EU parties – not counted in the official election campaign statements.

According to the 2020 report of the Alliance for Securing Democracy on covert foreign money[1], more than $300 million have already been funnelled into 33 countries over the past decade by Russia, China and other authoritarian regime to interfere in democratic processes more than 100 times, and half of these cases concern Russia's actions in Europe.

Some of these operations are not even illegal: they enjoy the many loopholes existing between the Member States whose provisions in the national electoral laws related to the financing of political activities are not harmonised at EU level.

Cyber security and resilience against cyber-attacks

The growing digitalisation of services has led to an increased reliance of critical infrastructures on online systems, thereby increasing the vulnerability to cyber-attacks and data exposure. The number of cyber-attacks has grown during recent years, targeting strategic sectors such as the European Medicines Agency (EMA) and the Norwegian Parliament.

Fragmented capacities and capabilities, and the low amount of human and financial resources, show the EU's vulnerability to cyber-attacks. Cyber-attacks do not stop at borders. It is therefore imperative the EU invests rapidly in its strategic digital capacities and capabilities - by allocating additional resources, both human and financial, to cybersecurity - while at the same time ensuring a common high level of cybersecurity is achieved across all Member States. The 2020 EU Cybersecurity Strategy and the NIS2 Directive are important proposals to improve the EU's cybersecurity, which will be strengthened in the future by the Cyber Resilience Act and the Cyber Defence Policy.

Furthermore, the issue with spy software, such as Pegasus, should be quickly addressed by reinforcing the legislative framework to hold the distributers, users and abusers of these software's accountable.

Protection of EU institutions

Cybersecurity should not only be improved across Member States, but also among the EU institutions. Recent cyber-attacks targeting the EU institutions have underlined the need for strong inter-institutional cooperation in terms of detecting, monitoring and sharing information during and/or to prevent cyber-attacks. The European institutions have already taken measures to strengthen its cybersecurity and have tools in place to coordinate and detect cyber-attacks, such as CERT-EU, ENISA and the upcoming Joint Cyber Unit.

However, more should be done. First of all, there should be an increase in both human and financial resources to meet the challenges of a constantly evolving threat landscape. Secondly,

[1] https://securingdemocracy.gmfus.org/covert-foreign-money/

the EU institutions should conduct a thorough review of its services and networks, to mitigate security risks and ensure the institutions are not dependent on foreign technologies for its security. And finally, awareness raising and proper training and guidance should be ensured amongst all staff to mitigate and address cyber, and non-cyber, security risks.

Interference through elite capture, national diasporas, universities

Another set of tools at the disposal of foreign countries willing to interfere in the functioning of the EU is the interference through people.

The 'elite capture' – or co-optation is unfortunately wide spread phenomenon, its most well known form is hiring former high-level European politicians and civil servants by companies controlled by foreign States in exchange of their knowledge acquired during public mandates or functions. Their knowledge, often based on confidential information and contacts, is then used at the expense of the EU and its Member States' strategic interests. These operations are often combined with industrial lobbying strategies, where economic and political goals are merged.

Another form of interference through people is the increasing influence and, ultimately control, of universities, schools as well as cultural and religious centres by foreign States agents, when it comes to topics relevant for the given foreign country. The way the Confucius Institutes - newly labelled 'Centers for Language Education and Cooperation' - are seeking to control all types of research, teaching or even cultural exhibition related to China within many European universities and museums is a vivid example of such practice. Other countries are also very active in this field, like for instance Russia through the orthodox churches.

This form of interference largely benefits from the efforts to control the national diaspora living within the EU, which represents a potential massive leverage throughout various layers of the European societies. These efforts also aim at silencing political opponents living abroad.

Deterrence and collective sanctions

The EU and its Member States need to set up credible deterrence tools. As a matter of fact, the EU and its Member States do not currently have any specific regime of sanctions related to foreign interference and disinformation campaigns orchestrated by foreign State actors.

The rapporteur is aware of the legal challenges that can emerge in establishing such sanctions regime, including the need to define precisely the elements of the crimes and their possible cumulative effects in conformity with EU and international laws.

The rapporteur considers however that the EU can get useful inspiration from what has been done by other partners in this regard, like Australia did in particular when defining what is a 'intentional foreign interference' and when criminalising covert and deceptive activities of foreign actors.

The rapporteur also thinks that we can build on what exists already at the EU level, notably the restrictive measures regime against cyber-attacks threatening the Union and its Member States, which have been used twice last year.

Last but not least, we emphasise the need to closely cooperate with our international like-

minded partners on any sanctions regime with the aim at imposing sanctions together in order to reinforce efficiency and deterrence effect.

Foreign entities responsible for aggressive interference operations against democracies should not assume that their destabilisation campaigns will meet no consequences.

Global cooperation and multilateralism

The EU is far from being the only democratic area in the world facing increasing aggressive foreign interference actions. Many other countries - whether developed or developing countries - are also targeted by such operations, from China or Russia and other authoritarian regimes, which pursue always the same goals: undermining democratic functioning in order to gain influence.

We need to bring together like-minded partners to tackle these issues in a coordinated way, based on a partnership of democracies.

First, we need to agree on common definitions and share understanding regarding what is currently at stake with a view to agree on international norms and standards.

The following questions should be precisely and collectively addressed and answered: What is an aggressive foreign interference? How to legally qualify disinformation and manipulation operations orchestrated from a foreign country? How can we define these threats and attacks as crimes? Which collective sanctions regime could be put in place?

Then, the global cooperation should be based on exchange of best practices and management of concrete projects. The European Parliament, through its vast network of inter-parliamentary fora, would have a leading role to pay here, as well as the EU delegations in third countries.

Working methods

No matter our political view on different pieces of legislation and our colours on the political spectrum, as INGE Members, we are united in the view that our democracy need to stand strong against foreign interference attempts. For this reason, we have built our work in the committee on deep cooperation between political groups. Coordinators decided jointly with the Chair which experts to invite and which studies to commission. As a rapporteur, I have regularly consulted the shadow rapporteurs during my drafting work.

Thematic-wise, we can distinguish the diagnosis phase from the solution-focused phase. During the first phase, we invited experts who could help us understand the threats and methods in all their varieties. Guided by the mandate, we had a number of hearings about interference in the public and private sphere and investigating the methods of different foreign actors. In the solution-focus phased, INGE focused on identifying possible tools and strategies to prevent and counter the identified problems.

INGE also commissioned six studies and invited the authors to present their findings. The sanitary situation linked to the Covid-19 pandemic prevented us from organising any missions during the first two semesters of INGE's existence. At the time of writing this, however, INGE members just came back from a first successful mission to the European Union Agency for Cybersecurity (ENISA) in Athens, Greece. Three further missions are planned: to Taipei,

Paris and Washington.

To further prepare our recommendations, we drafted two questions for oral answers. In July 2021, we asked VP/HR Josep Borrell how he intended to remedy the lack of resources and mandate for the EEAS Stratcom Taskforces and the lack of proper sanctions against foreign actors engaging in interference. In October 2021, we asked Commission Vice-President Věra Jourová how she plans to ensure that lack of coordination across sectors and political levels does not increase the exposure for foreign interference and how to improve algorithm transparency and support media literacy.

One of our key conclusions was the importance of cooperation and information sharing, both globally and between levels of governance and different sectors within the EU. From the beginning, we have therefore invited other committees and delegations with competences linked to foreign interference to our meetings. The expertise from these sister bodies enriched the debates we had with invited guests and made sure that the insights from our hearings land in the ordinary committees working with corresponding legislative proposals.

One key event will be the inter-parliamentary meeting we will host in November 2021. This meeting between parliamentarians from EU countries and a selected group of like-minded global partners will be a crucial opportunity to learn from each other and discuss common challenges and solutions.

To prepare this report, the rapporteur drafted four working documents: on the state of the foreign interference in the European Union, including disinformation, on covert funding of political activities by foreign donors, on foreign interference using online platforms and on building EU resilience against hybrid threats.

In addition to all mentioned formal meetings, the rapporteur collected knowledge through meetings, participation in conferences and extensive reading of studies and news articles.

Cooperation with other European Parliament bodies and EU bodies

Due to the cross-sector nature of our mandate, INGE invited and discussed different aspects of foreign interference with five Commissioners:

- Věra Jourová, Vice-President for Values and Transparency,
- Margaritis Schinas, Vice-President for Promoting our European Way of Life,
- Josep Borrell, Vice-President of the European Commission/ High Representative of the Union for Foreign Affairs and Security Policy,
- Thierry Breton, Commissioner for Internal Market, and
- Margrethe Vestager, Executive Vice-President for A Europe Fit for the Digital Age and Competition,

We also had several discussions with staff from of the Commission and the External Action Services and a special meeting, together with CONT, with the European Court of Auditor about its Special Report 09/2021: Disinformation affecting the EU: tackled but not tamed.

The INGE Special Committee has also established a cooperation plan with several EP

Committees with which it shares some remit of competence. INGE has so far eleven committees and eleven delegations.

External expertise

The Special Committee on Foreign Interference in all Democratic Processes in the EU, including Disinformation, has requested the external expertise on the following topics that are relevant to the committee's ongoing work:

- Disinformation - mapping and solutions, including regulating the platforms
- Financing - mapping and solutions
- Infrastructures
- Best practices in the whole of society approach in countering hybrid threats.
- Impact of disinformation campaigns on migrants, LGBTI and minority groups.
- Lessons learnt from misuse by authoritarian regimes.

Overview of hearings with external experts

Thematic hearings

- **Hybrid threats, disinformation and polarisation – institutional overview**, 24 September 2020
- **Electoral interference, political parties funding and social media platforms – overview**, 2 October 2020
- **How foreign interference undermines sovereignty: our Eastern neighbours' example**, 21 October 2020
- **Foreign interference in the public sphere: Fact-checking, social media platforms and their use in disinformation and foreign interference and resilience-building**, 26 October 2020 and 9 November 2020
- **Foreign interference in the political sphere: Foreign interference during electoral processes, including through cyber-attacks, data leaks and malign communication**, 12 November 2020
- **Foreign interference in the political sphere: Political funding by legal or illegal forms of conduits and straw donors from third-country sources**, 2 December 2020
- **Journalism vs propaganda**, 11 December 2020
- **Possible threats of interference from third countries in a geopolitical context**, 25 January 2021 and 1 February 2021
- **Strategic communication to counter foreign interference**, 22 February 2021

- **How to make political party and campaign financing more transparent: what rules do we need in the EU?**, 23 February 2021,
- **Democracy Online: what are the risks? How to protect us?**, 17 March 2021
- **Foreign interference on the financing of anti-choice organisations in the EU**, 25 March 2021,
- **Tech developments and regulatory approaches to disinformation: Interference through advertisement**, 13 April 2021,
- **Tech Developments and Regulatory Approaches regarding Disinformation**, 15 April 2021
- **Exchange of views with Mikhail Khodorkovsky, founder of Dossier Center**, 10 May 2021,
- **Hearing with Facebook, Twitter and Youtube on the Role of Social Media Platforms for spreading and developing disinformation and for detecting and countering it**, 10 May 2021,
- **How history, culture and education can help counter disinformation**, 15 June 2021,
- **Disinformation and discrimination**, 12 July 2021
- **The European Democracy Action Plan and Digital Services Act and other EU instruments: how the proposals could protect democratic processes in the EU against foreign interference, and the way forward**, 2 September 2021
- **Sanctions and collective countermeasures**, 2 September 2021

Exchange of views with

- **The role of education, media and culture in addressing disinformation and foreign interference**, 9 September 2021,
- **Foreign interference and spying on European politicians and institutions**, 9 September 2021,
- **Security of EU institutions: responding to the escalation in cyberattacks**, 9 September 2021,
- **Economic damage of foreign interference/disinformation, including the data market**, 14 October 2021.