EPP Group Conclusions of the

INGE* + ING2**

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

** "Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation, and the Strengthening of Integrity, Transparency and Accountability in the European Parliament"

epp group
in the european parliament

INDEX

FOREWORD, MANFRED WEBER MEP

Manfred Weber MEP
Chairman of the EPP Group
in the European Parliament

Dear friends,

It is with great pleasure that I present to you this publication on the important work of two Special Committees in the European Parliament focused on foreign interference (INGE and ING2).

These two committees were established with the idea that in a rapidly evolving world with big geopolitical changes and permanent technological advancements, the EPP Group is fully committed to protecting the principles of democracy and ensuring the integrity of our democratic processes.

Recognising the pressing need to confront the challenges posed by foreign interference, the INGE-Committee was established with its main mission to fight disinformation. The work of the Special Committee has been vital in highlighting the need for us to do more to protect our democratic institutions. For the EPP Group, it is clear that the EU must strengthen its own capacities to detect, expose and fight disinformation. We have to invest more to safeguard our democracy in the context of a comprehensive and coordinated European strategy.

Building on the foundation laid by INGE, we recognised the continued significance of this endeavour and established its successor ING2 to also screen existing and planned EU legislation in a range of areas for loopholes that could be exploited by third countries for malicious purposes.

With the knowledge gained through the efforts of INGE and ING2, we are more aware of the threats that are out there and more prepared to protect ourselves against them.

I would like to thank the EPP Group members of the Special Committees, who have done very important work to make sure our EPP Group priorities were integrated in the reports as well as the staff who accompanied the work of the Special Committees.

Javier Zarzalejos MEP
First Vice-Chair INGE and ING2

INTRODUCTION, JAVIER ZARZALEJOS MEP

In recent years, the EU has realised the enormous challenge that foreign interference and disinformation campaigns deployed from abroad represent for democracy. The institutions have developed measures to fight against these types of strategies that seek to undermine the basic pillars on which our democratic system is built and sustained.

During the current legislature, the European Parliament established the Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE) to define an approach that addresses evidence of foreign interference in the EU and its Member States.

More broadly, this committee not only aims to protect the values of the European Union, but democracy itself. The quality of our democracies leans on citizens making informed decisions, which makes the fight against disinformation and foreign interference a priority.

On 9 March, the European Parliament's plenary adopted the first report on this issue, analysing the situation in the EU and setting out concrete recommendations to combat such actions. The report notes that Russia, China and other authoritarian regimes, such as Iran and Venezuela, have funnelled "more than 259 million euros into 33 countries to interfere in democratic processes, and this trend is clearly accelerating".

On June 1, the Parliament adopted a new report following up on the implementation of the Resolution adopted in March 2022. The text highlights interference on online platforms, protection of critical infrastructure and strategic sectors, interference during electoral processes, covert funding of political activities by foreign actors and resilience to cyberattacks. The report focuses particularly on Russian and Chinese interference in the EU, in countries applying to join the EU, including the Western Balkans, and countries in the Global South.

In these reports, Russia is singled out as being responsible for major interference and disinformation campaigns on European soil. There is evidence of Russian interference in European democracies, such as the Brexit referendum in the United Kingdom, the secessionist process in Catalonia, the 2017 presidential elections in France, as well as practical support for extremist, populist and anti-European parties across Europe, particularly in France, Germany, Italy and Austria. Russia's goal in all these cases has always been the same: to promote internal destabilisation and disunity in the European Union. In addition, Russia's war against Ukraine has been paved by disinformation.

Today, disinformation strategies are becoming increasingly sophisticated, fueled by the rapid development of technology. The EU must address this growing security threat and take the necessary measures. It must strengthen its own capabilities to detect, expose and combat disinformation and all types of hybrid threats. It is essential to implement a coordinated strategy that outlines new initiatives and improves the implementation of existing ones. Better funding is also needed, and measures put in place to protect the integrity of the upcoming European elections. These are vital tasks for the EU, with the ultimate aim of protecting the principles and values on which our democracies are established.

INTRODUCTION, VLADIMÍR BILČÍK MEP

Vladimír Bilčik MEP
Coordinator for the EPP Group
INGE and ING2

I am proud of the many things that my colleagues and I have achieved in our parliamentary work during this mandate. In particular, our work in the INGE Committee. For me, this committee is proof that we can collectively formulate effective responses to longstanding, serious issues that were previously overlooked and will continue to pose significant dangers in the future.

The establishment of the committee also came at the right time and brought together representatives from countries and political groups who were united by sincere interest and shared desire to find ways to defend our society from harmful influence and actions by malicious actors.

As we approach European elections in 2024 the EU is much more aware of the threats that foreign interference poses to European democracy. We are better able to identify the pernicious consequences of disinformation on our society. We are familiar with the fact that as a result of their business model large online platforms systematically contribute to fear and anxiety among people. We know that deliberate, well-organised, coordinated and dangerous campaigns exist in both the online and offline world. More than anyone else, the people of Ukraine, and also of other vulnerable countries such as Moldova, are painfully aware of these phenomena. We know that at the end of such campaigns, in extreme cases people end up fighting for their bare lives.

This picture of our reality was not at all that clear just a few years ago. I am therefore very proud of the work that we achieved in the INGE Committee. Together, we managed to gather the best available and up to date expert knowledge. Dozens of hearings helped us create a detailed map of the challenges that we are facing.

Thanks to the work of all our colleagues, and I dare say proudly that especially our colleagues from the EPP Group, we have managed not only to describe accurately the pitfalls of malign foreign interventions in our democracy, but we have also helped turn this once marginal topic into a fixed part of deliberations about the EU's external and internal security policies.

Our task now is to reinforce this public attention and come up with answers and solutions to the constantly evolving risks of foreign interference and disinformation. Thanks to the team that we managed to create in the EPP Group, I have no doubt that we are going to succeed.

Sandra Kalniete MEP
Rapporteur INGE and ING2

CONTRIBUTION, SANDRA KALNIETE MEP, RAPPORTEUR INGE AND ING2

As the rapporteur for INGE1 and ING2, I had the privilege to lead the work on two different but equally important documents.

The Special Committee's first report was adopted just 2 weeks after the brutal invasion of Ukraine by Russia. This was an eye-opening moment for many – Putin's propaganda machinery was not only "turned on" only on 24 February, it has already been working for decades in Europe, attempting to poison and divide our societies. We have arrived at the moment of truth to ask frank questions - How did the democratic world get to this point? How can we prevent it in the future?

INGE1 has provided both the diagnosis of the EU's vulnerabilities and prescribes the medication for strengthening the EU's resilience.

The report identified and mapped the threat of foreign interference in all of its forms, including disinformation, manipulation of social media platforms and advertising systems, cyberattacks, threats against and the harassment of journalists. Another crucial factor weakening our resilience is foreign covert funding, elite capture and co-optation. For decades, we have watched former high-ranking European officials and politicians take up prominent positions in Russian energy companies, while we were channelling hundreds of millions into Putin`s coffers and providing a safe haven for his cronies and oligarchs.

In the second phase of the committee work-ING2 was devoted to the assessment of the existing tools tackling foreign information manipulation and putting forward tailored recommendations. The overall conclusion is that we need stronger measures and better coordination to protect democracy, also given the upcoming EU elections in 2024.

First, we need more sustainable and long-term investment in our civil society organisations tackling information manipulation. They have proved that their work can make an impact. Although there are many valuable projects and initiatives, the funding is still project-based, often relying on third-country sources and not covering basic administrative costs or requiring an unrealistic share of co-financing. Therefore, we need a dedicated EU programme to invest in our democracy sustainably. It will pay off in the long term.

Another important conclusion of the ING2 report is that in tackling disinformation, the EU is still suffering from a very fragmented approach, without clear coordination mechanisms and goals. We simply cannot afford compartmentalisation when our democracy and integrity may be at stake- particularly now, when we are facing the rapid development of the artificial intelligence tools, we will need more agile ways to tackle the disinformation.

In addition to building our resilience, we should expose the preparatory to the costs: deliberately and intentionally engaging in foreign information manipulation should be a highly expensive and damaging exercise for any state or non-state player. Therefore, the toolbox of the EU countermeasures should include a specific permanent sanctions regime on foreign information manipulation and interference.

Russia's war of aggression against Ukraine clearly exposed the interconnection between attempts at foreign information manipulation and threats to the EU, its immediate neighbourhood, Western Balkans and Eastern Partnership countries, as well as to global security and stability. The EU should not stop at scratching the surface and admiring the problem. Bringing our fight against foreign interference and information manipulation at the new level is our common task for the upcoming months and years.

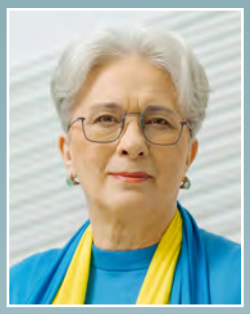
INGE

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

EPP GROUP MEMBERS OF THE EUROPEAN PARLIAMENT'S SPECIAL COMMITTEE (INGE)

Javier ZARZALEJOS
First Vice-Chair

Vladimír BILČÍK
Coordinator



Sandra KALNIETE
Member, Rapporteur

Ioan-Rareş BOGDAN
Member

Sunčana GLAVAK
Member

Andrey KOVATCHEV
Member

Jeroen LENAERS
Member

Lukas MANDL
Member

Sabine VERHEYEN
Member

Magdalena ADAMOWICZ
Substitute

Salvatore DE MEO
Substitute

Frances FITZGERALD
Substitute

Rasa JUKNEVIČIENĖ
Substitute

David McALLISTER
Substitute

Nuno MELO
Substitute

Eugen TOMAC
Substitute

Iuliu WINKLER
Substitute

Tomáš ZDECHOVSKÝ
Substitute

FINAL REPORT INGE

TEXTS ADOPTED

P9_TA(2022)0064

Foreign interference in all democratic processes in the European Union
European Parliament resolution of 9 March 2022 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 ('the Charter'), and in particular Articles 7, 8, 11, 12, 39, 40, 47 and 52 thereof,

- having regard to the Charter of the United Nations, in particular Articles 1 and 2 thereof,

- having regard to United Nations General Assembly Resolution 2131 (XX) of 21 December 1965 entitled 'Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty',

- having regard to the Convention for the Protection of Human Rights and Fundamental Freedoms, and in particular Articles 8, 9, 10, 11, 12, 13, 14, 16 and 17 thereof, and to the Protocol thereto, and in particular Article 3 thereof,

- having regard to its resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties[1] and to its recommendation of 13 March 2019 concerning taking stock of the follow-up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda against it by third parties[2],

- having regard to its resolution of 13 June 2018 on cyber defence[3] ,

- 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 joint staff working document of 23 June 2021 on the Fifth Progress Report on the implementation of the 2016 Joint Framework on countering hybrid threats

1 OJ C 224, 27.6.2018, p. 58.
2 OJ C 23, 21.1.2021, p. 152.
3 OJ C 28, 27.1.2020, p. 57.

and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats (SWD(2021)0729),

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

- having regard to the Commission communication of 3 December 2020 entitled 'Europe's Media in the Digital Decade: An Action Plan to Support Recovery and Transformation' (COM(2020)0784),

- having regard to the Digital Services Act package,

- having regard to its resolution of 20 October 2021 entitled 'Europe's Media in the Digital Decade: an Action Plan to Support Recovery and Transformation'[1],

- having regard to the 2018 Code of Practice on Disinformation and the 2021 Guidance on Strengthening the Code of Practice on Disinformation (COM(2021)0262), and to the Recommendations for the New Code of Practice on Disinformation issued by the European Regulators Group for Audiovisual Media Services in October 2021,

- 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[2] (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 International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts,

- 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),

- 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)

---

1 Texts adopted, P9_TA(2021)0428.

2 OJ L 79 I, 21.3.2019, p. 1.

and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013[1],

– having regard to the studies, briefings and in-depth analysis requested by the Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE),

– having regard to the Frances Haugen hearing of 8 November 2021 organised by its Internal Market and Consumer Protection Committee, in association with other committees,

– having regard to its resolution of 7 October 2021 on the state of EU cyber defence capabilities[2],

– having regard to the United Nations Sustainable Development Goals (SDGs), and in particular to SDG 16 which aims to promote peaceful and inclusive societies for sustainable development,

– having regard to the State of the Union 2021 address and letter of intent,

– having regard to the UN Secretary-General's report of 10 September 2021 entitled 'Our Common Agenda',

– having regard to the joint communication from the Commission and the High Representative of the Union for Foreign and Security Policy of 10 June 2020 entitled 'Tackling COVID-19 disinformation – Getting the facts right' (JOIN(2020)0008),

– having regard to the Council's decision of 15 November 2021 to amend its sanction regime on Belarus to broaden the designation criteria to target individuals and entities organising or contributing to hybrid attacks and the instrumentalisation of human beings carried out by the Belarus regime,

– 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 (A9-0022/2022),

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;

---

1 OJ L 151, 7.6.2019, p. 15.
2 Texts adopted, P9_TA(2021)0412.
3 OJ C 362, 8.9.2021, p. 186.

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 and threaten these freedoms, as well as undermining democratic processes in the EU and its Member States, such as the holding of free and fair elections; whereas the objective of foreign interference is to distort or falsely represent facts, artificially inflate one-sided arguments, discredit information to degrade political discourse and ultimately undermine confidence in the electoral system and therefore in the democratic process itself;

C. whereas Russia has been engaging in disinformation of an unparalleled malice and magnitude across both traditional media outlets and social media platforms, in order to deceive its citizens at home and the international community on the eve of and during its war of aggression against Ukraine, which Russia started on 24 February 2022, proving that even information can be weaponised;

D. whereas any action against foreign interference and information manipulation must itself respect the fundamental freedoms of expression and information; whereas the EU Fundamental Rights Agency (FRA) plays a key role in evaluating respect for fundamental rights, including Article 11 of the Charter, in order to avoid disproportionate actions; whereas actors carrying out foreign interference and information manipulation misuse those freedoms to their advantage and it is therefore vital to step up the precautionary fight against foreign interference and information manipulation because democracy depends on people making informed decisions;

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

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

G. whereas foreign interference tactics take many forms, including disinformation, the suppression of information, the manipulation of social media platforms and their algorithms, terms and conditions, and advertising systems, cyberattacks, hack-and-leak operations to gain access to voter information and interfere with the legitimacy of the electoral process, threats against and the harassment of journalists, researchers,

politicians and members of civil society organisations, covert donations and loans to political parties, campaigns favouring specific candidates, organisations and media outlets, fake or proxy media outlets and organisations, elite capture and co-optation, 'dirty' money, fake personas and identities, pressure to self-censor, the abusive exploitation of historical, religious and cultural narratives, pressure on educational and cultural institutions, taking control of critical infrastructure, pressuring foreign nationals living in the EU, the instrumentalisation of migrants and espionage; whereas these tactics are often combined for greater effect;

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

I. whereas misinformation is verifiably false information which is not intended to cause harm, while disinformation is verifiably false or misleading information that is intentionally created, presented or disseminated with a view to causing harm or producing a potentially disruptive effect on society by deceiving the public or for intentional economic gain;

J. whereas there is a need to agree within the EU on common and granular definitions and methodologies to improve the shared understanding of the threats and develop appropriate EU standards for improved attribution and response; whereas the European External Action Service (EEAS) has done a considerable amount of work in this area; whereas these definitions must guarantee imperviousness to external interference and respect for human rights; whereas cooperation with like-minded partners, in relevant international forums, on common definitions of foreign interference in order to establish international norms and standards is of the utmost importance; whereas the EU should take the lead in establishing clear international rules for the attribution of foreign interference;

Need for a coordinated strategy against foreign interference

K. whereas foreign interference attempts across the world are increasing and becoming more systemic and sophisticated, relying on widespread use of artificial intelligence (AI) and eroding attributability;

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

M. whereas there is a general lack of awareness among many policy-makers, and citizens in general, of the reality of these issues, which may unintentionally contribute to opening up further vulnerabilities; whereas the issue of disinformation campaigns has not been at the top of the agenda of European policy-makers; whereas the hearings and work of the INGE Special Committee have contributed to public recognition and the

contextualisation of these issues and have successfully framed the European debate on foreign interference; whereas long-lasting foreign disinformation efforts have already contributed to the emergence of home-grown disinformation;

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

O. whereas the first priority of EU defence, i.e. the resilience and preparedness of EU citizens vis-à-vis foreign interference and information manipulation, requires a long-term and whole-of-society approach, beginning with education and raising awareness of the problems at an early stage;

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

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

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

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

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

T. whereas different stakeholders and institutions use different methodologies and definitions to analyse foreign interference – all with different degrees of comprehensibility, and whereas these differences can inhibit comparable monitoring,

analysis and assessment of the threat level, which makes joint action more difficult; whereas there is a need for an EU definition and methodology to improve the common threat analysis;

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

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

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

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

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

Z. whereas next to state institutions, journalists, opinion leaders and the private sector, each section of society and each individual have important roles to play in identifying and putting a stop to the spread of disinformation and in warning people in their environment who are at risk; whereas civil society, academia and journalists have already contributed strongly to raising public awareness and increasing societal resilience, including in cooperation with counterparts in partner countries;

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

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

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

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

Foreign interference using online platforms

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

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

AG. whereas in response to Russia's war of aggression against Ukraine, the Prime Ministers of Estonia, Latvia, Lithuania and Poland sent a letter to the CEOs of the Big Tech social media platforms (Twitter, Alphabet, YouTube and Meta) on 27 February 2022, calling for, inter alia, the suspension of accounts engaging in and glorifying war crimes and crimes against humanity, reinforced content moderation in the Russian and Ukrainian languages, the full and immediate demonetisation of all accounts disseminating disinformation perpetrated by the Russian and Belarusian Governments, and assistance for users trying to find trustworthy information on the war in Ukraine;

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

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

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

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

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

AM. whereas algorithm curation mechanisms and other features of social media platforms are engineered to maximise engagement; whereas these features are repeatedly reported

to promote polarising, radicalising and discriminatory content and keep users in like-minded circles; whereas this leads to the gradual radicalisation of platform users, as well as the conditioning and polluting of collective discussion processes, rather than the protection of democratic processes and individuals; whereas uncoordinated actions by platforms have led to discrepancies in their actions and allowed disinformation to spread from platform to platform; whereas the business model of making money through the spread of polarising information and the designing of algorithms make platforms an easy target for manipulation by foreign hostile actors; whereas social media platforms could be designed differently so as to foster a healthier online public sphere;

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

AO. whereas self-regulation systems such as the 2018 Code of Practice on Disinformation have led to improvements; whereas, however, relying on the goodwill of platforms is neither working nor effective and has produced little meaningful data on their overall impact; whereas, in addition, platforms have taken individual measures varying in degree and effect, leading to backdoors through which content can continue to spread elsewhere despite being taken down; whereas there needs to be a clear set of rules and sanctions in order for the Code of Practice to have sufficient effect on the online environment;

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

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

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

AS. whereas platforms' complaint and appeal procedures are generally inadequate;

AT. 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;

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

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

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

Critical infrastructure and strategic sectors

AX. whereas the management of threats to critical infrastructure, 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;

AY. 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 services will be set out in the annex to the directive;

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

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

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

Foreign interference during electoral processes

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

BD. whereas the distinctive nature of foreign interference in electoral processes, and the use of new technologies in this regard, as well as their potential effects, represent especially dangerous threats to democracy; whereas foreign interference in electoral processes goes well beyond social media 'information warfare', favouring specific candidates to hack and target databases and gain access to the information of registered voters and directly interfering with the normal functioning, competitiveness and legitimacy of the electoral process; whereas foreign interference aims to introduce doubt, uncertainty and mistrust, and not just to alter the result of elections but to delegitimise the entire electoral process;

Covert funding of political activities by foreign actors and donors

BE. whereas a 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;

BF. 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 other actors such as Iran and Venezuela, from the Middle-East and on the US far right have also been involved in covert funding; whereas this trend is clearly accelerating; whereas half these cases concern Russia's actions in Europe; whereas corruption and illicit money laundering are a source of political financing from authoritarian third countries;

BG. whereas media tools created by foreign donors in a non-transparent way have become highly effective in garnering large numbers of followers and generating engagement;

BH. whereas these operations finance extremist, populist, anti-European parties and certain other parties and individuals or movements seeking to deepen societal fragmentation and undermine the legitimacy of European and national public authorities; whereas this has helped to increase the reach of these parties and movements;

BI. whereas Russia seeks out contacts to parties, figures and movements in order to use players within the EU institutions to legitimise Russian positions and proxy governments, to lobby for sanctions relief and to mitigate the consequences of international isolation; whereas parties such as the Austrian Freiheitliche Partei Österreichs, the French Rassemblement National and the Italian Lega Nord have signed cooperation agreements with Russian President Vladimir Putin's United Russia party and now face media allegations of being willing to accept political funding from Russia; whereas other European parties such as the German Alternative für Deutschland (AfD), the Hungarian Fidesz and Jobbik, and the Brexit Party in the UK also reportedly have close contact with the Kremlin, and the AfD and Jobbik have also worked as so-called 'election observers' in Kremlin-controlled elections, for example in Donetsk and Lugansk in eastern Ukraine, to monitor and legitimise Russian-sponsored elections; whereas findings about the close and regular contacts between Russian officials and representatives of a group of Catalan secessionists in Spain, as well as between Russian officials and the largest private donor for the Brexit Vote Leave campaign, require an in-depth investigation, and are part of Russia's wider strategy to use each and every opportunity to manipulate discourse in order to promote destabilisation;

BJ. whereas the Group of States against Corruption (GRECO) of the Council of Europe and the Venice Commission have already made wide-ranging recommendations to decrease the scope for the possible interference of foreign actors via political financing;

BK. whereas electoral laws, in particular provisions on the financing of political activities, are not sufficiently well coordinated at EU level, and therefore allow for opaque financing methods by foreign actors; whereas the legal definition of political donations is too narrow, allowing for foreign in-kind contributions in the European Union;

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

BM. whereas lack of financing transparency creates an environment for corruption, which often accompanies foreign funding and investments;

BN. whereas Regulation (EU, Euratom) No 1141/2014 of 22 October 2014 on the statute and funding of European political parties and European political foundations[1] is being revised with a view to achieving a greater level of transparency in terms of the financing of political activities;

BO. whereas the role of political foundations has grown in recent years, in most cases playing a positive role in politics and in strengthening democracy, but in some cases becoming a more unpredictable vehicle for malicious forms of finance and indirect interference;

BP. whereas modern technologies and digital assets, such as cryptocurrency, are used to disguise illegal financial transactions to political actors and political parties;

Cybersecurity and resilience against cyberattacks

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

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

BS. whereas the Member States have increased their cooperation in the domain of cyber defence within the framework of the Permanent Structured Cooperation (PESCO), including by setting up Cyber Rapid Response Teams; whereas the European Defence Industrial Development Programme (EDIDP) has included intelligence, secured communication and cyber defence in its work programmes; whereas the current capacity to face cyber threats is limited owing to the scarcity of human and financial

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

resources, for example in critical structures such as hospitals; whereas the EU has committed to investing EUR 1.6 billion, under the Digital Europe programme[1], in the response capacity and deployment of cybersecurity tools for public administrations, businesses and individuals, as well as developing public-private cooperation;

BT. whereas gaps in and the fragmentation of the EU's capabilities and strategies in the cyber field is becoming an increasing problem, as pointed out by the European Court of Auditors[2]; whereas the EU Cyber Diplomacy Toolbox, set up in May 2019, has shown the added value of a joint EU diplomatic response to malicious cyber activities; whereas the Council decided for the first time on 30 July 2020 to impose restrictive measures on individuals, entities and bodies responsible for or involved in various cyberattacks;

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

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

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

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

BX. 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 preventing them, including during EU common security and defence policy (CSDP) missions and operations; whereas the EU and its Member States should organise regular, joint exercises to identify weak spots and take the necessary measures;

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

BY. whereas a number of politicians, including former high-level European politicians and civil servants are hired or co-opted by foreign authoritarian state-controlled national or private companies in exchange for their knowledge and at the expense of the interests of the citizens of the EU and its Member States;

BZ. whereas some countries are particularly active in the field of elite capture and co-optation, in particular Russia and China, but also Saudi Arabia and other Gulf countries, with, for instance, former German Chancellor Gerhard Schröder and former Prime

---

1 https://www.consilium.europa.eu/en/policies/cybersecurity/

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

Minister of Finland Paavo Lipponen having both joined Gazprom to speed up the application process for Nord Stream 1 and 2, former Austrian Minister of Foreign Affairs Karin Kneissl appointed board member of Rosneft, former Prime Minister of France François Fillon appointed board member of Zaroubejneft, former Prime Minister of France Jean-Pierre Raffarin actively engaged in promoting Chinese interests in France, former Czech Commissioner Štefan Füle having worked for CEFC China Energy, former Prime Minister of Finland Esko Aho now on the board of the Kremlin's Sberbank, former French Minister for Relations with Parliament Jean-Marie Le Guen now a member of the Board of Directors of Huawei France, former Prime Minister of Belgium Yves Leterme appointed Co-Chairman of the Chinese investment fund ToJoy, and many other high-level politicians and officials taking on similar roles;

CA. whereas economic lobbying strategies can be combined with foreign interference goals; whereas according to the OECD's report on lobbying in the 21st century[1] only the US, Australia and Canada have rules in place that cover foreign influence; whereas there is a serious lack of legally binding rules and enforcement of the EU's lobbying register, which makes it practically impossible to track lobbying coming from outside the EU; whereas there is currently no way of monitoring lobbying efforts in Member States that influence legislation and foreign policy through the European Council; whereas rules on lobbying in the EU focus mainly on face-to-face contact and do not take into account the whole ecosystem of different types of lobbying that exists in Brussels; whereas countries such as China and Russia, but also Qatar, the United Arab Emirates and Turkey, have invested heavily in lobbying efforts in Brussels;

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

CC. whereas different state actors, such as the Russian, Chinese and, to a lesser degree, Turkish Governments, have been attempting to increase their influence by setting up and using cultural, educational (e.g. through grants and scholarships) and religious institutes across Member States, in a strategic effort to destabilise European democracy and expand control over Eastern and Central Europe; whereas the alleged difficult situation of its national minority has been used in the past by Russia as an excuse for direct intervention in third countries;

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

CE. whereas Russian state-controlled Sputnik and RT networks that are based in the West, combined with Western media and fully or partially owned by Russian and Chinese legal and individual entities actively engage in disinformation activities against liberal

[1] Organisation for Economic Co-operation and Development, Lobbying in the 21st Century: Transparency, Integrity and Access, 2021, OECD Publishing, Paris, available at: https://doi.org/10.1787/c6d8eff8-en

democracies; whereas Russia is resorting to historical revisionism, seeking to rewrite the history of Soviet crimes and promoting Soviet nostalgia among the susceptible population in Central and Eastern Europe; whereas for national broadcasters in Central and Eastern Europe it is difficult to compete with Russian-language TV content funded by the Russian Government; whereas there is a risk of unbalanced cooperation between Chinese and foreign media, taking into account that Chinese media are the voice of the Chinese Communist Party at home and abroad;

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

CG. whereas the EU is currently lacking the necessary toolbox to address elite capture and counter the establishment of channels of influence, including within EU institutions; whereas situational awareness capabilities and counter-intelligence instruments remain scarce at EU level, with a high degree of reliance on national actors' willingness to share information;

Deterrence, attribution and collective countermeasures, including sanctions

CH. 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;

CI. whereas ensuring clear attribution of disinformation and propaganda attacks, including publicly naming the perpetrators, their sponsors and the goals they seek to achieve, as well as measuring the effects of these attacks on the targeted audience, are the first steps towards effectively defending against such actions;

CJ. whereas the EU should strengthen its deterrence tools and tools for attributing such attacks and categorising their nature as violating or not violating international law, with a view to establishing an effective sanctions regime so that malicious foreign actors have to pay the costs of their decisions and bear the consequences; whereas targeting individuals might not be sufficient; whereas other tools, such as trade measures, could be used to protect European democratic processes against state-sponsored hybrid attacks; whereas deterrence measures must be applied transparently with all due guarantees; whereas hybrid attacks are calibrated so that they deliberately fall below the threshold of Article 42(7) of the Treaty on European Union (TEU) and Article 5 of the North Atlantic Treaty;

Global cooperation and multilateralism

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

CL. whereas the EU accession countries in the Western Balkans are being hit particularly hard by attacks in the form of foreign interference and disinformation campaigns

stemming from Russia, China and Turkey, such as Russia's interference campaigns during the ratification process of the Prespa Agreement in North Macedonia; whereas the COVID-19 pandemic has been further exploited in the Western Balkans by China and Russia to destabilise these countries and discredit the EU; whereas candidate and potential candidate countries are expected to join the EU's initiatives to fight foreign interference;

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

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

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, conducted overwhelmingly by Russia and China and targeting all parts of the democratic functioning of the European Union and its Member States;

2. Welcomes the Commission President's announcement of 27 February 2022 of an EU-wide ban on Russian propaganda outlets such as Sputnik TV, RT (formerly known as Russia Today) and other Russian disinformation organs which have the sole aim of weakening and dividing the EU's public opinion and EU decision-makers; calls for further measures in this regard;

3. Calls on the Commission to propose, and the co-legislators and Member States to support, a multi-layer, coordinated and cross-sector strategy, as well as adequate financial resources, aimed at equipping the EU and its Member States with appropriate foresight and resilience policies and deterrence tools, enabling them to tackle all hybrid threats and attacks orchestrated by foreign state and non-state actors; considers that this strategy should be built on:

   (a) common terminologies and definitions, a single methodology, evaluations and ex post impact assessments of the legislation adopted so far, a shared intelligence system, and understanding, monitoring, including early warnings, and situational awareness of the issues at stake;

   (b) concrete policies enabling resilience-building among EU citizens in line with democratic values, including through support to civil society;

(c) appropriate disruption and defence capabilities;

(d) diplomatic and deterrence responses, including an EU toolbox for countering foreign interference and influence operations, including hybrid operations, through adequate measures, e.g. attribution and naming of perpetrators, sanctions and countermeasures, and global partnerships to exchange practices and promote international norms of responsible state behaviour;

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

5. Considers that this strategy should be based on a risk-based, whole-of-society and whole-of-government approach, covering the following areas in particular:

(a) building EU resilience through situational awareness, media and information literacy, media pluralism, independent journalism and education,

(b) foreign interference using online platforms;

(c) critical infrastructure and strategic sectors;

(d) foreign interference during electoral processes;

(e) covert funding of political activities by foreign actors and donors;

(f) cybersecurity and resilience against cyberattacks;

(g) protection of EU Member States, institutions, agencies, delegations and missions;

(h) interference through global actors via elite capture, national diasporas, universities and cultural events;

(i) deterrence, attribution and collective countermeasures, including sanctions;

(j) global cooperation and multilateralism;

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

7. Is concerned about the overwhelming lack of awareness, including among the broader public and government officials, of the severity of the current threats posed by foreign authoritarian regimes and other malicious actors targeting all levels and sectors of

European society, aimed at undermining fundamental rights and public authorities' legitimacy, deepening political and social fragmentation and, in some instances, even causing life-threatening harm to EU citizens;

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

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

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

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

12. Notes that a number of long-term projects and programmes with a focus on countering disinformation at a technological, legal, psychological and informational level are being funded by the EU; calls on the Commission to assess the impact of these projects and programmes and their applicability;

13. Calls on the Commission to set up a Commission taskforce led byVěra Jourová, as Vice-President of the Commission for Values and Transparency, dedicated to scrutinising existing legislation and policies to identify gaps that could be exploited by malicious actors, and urges the Commission to close these gaps; stresses that this structure should cooperate with other EU institutions and Member States at national, regional and local level and facilitate the exchange of best practices; calls on the Commission and the EEAS to consider the establishment of a well-resourced and independent European Centre for Interference Threats and Information Integrity, which should identify, analyse and document information manipulation operations and interference threats against the EU as a whole, increase situational awareness, develop a specialised knowledge hub by becoming a platform for coordination with civil society, the business sector, the EU and national institutions, and raise public awareness, inter alia via regular reports on systemic threats; stresses that the tentative creation of such a new independent and well-resourced European Centre for Interference Threats and

Information Integrity should clarify and enhance the role of the EEAS StratCom division and its taskforces as the strategic body of the EU's diplomatic service and prevent the overlap of activities; stresses that EEAS StratCom's mandate should be focused on strategically developing external policies to counter existing and emerging joint threats and to enhance engagement with international partners in this field; points out that EEAS StratCom could pursue this in close cooperation with a new European Centre for Interference Threats and Information Integrity and a new Commission taskforce;

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

Building EU resilience through situational awareness, media literacy and education

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

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

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

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

19. Underlines that public diplomacy and strategic communication are essential elements of the EU's external relations and the protection of the EU's democratic values; calls for the EU institutions to further develop and boost the important work of the EEAS StratCom division, with its taskforces, EU Intelligence and Situation Centre (EU

INTCEN) and Hybrid Fusion Cell, the EU Military Staff Intelligence Directorate, the Rapid Alert System, the established cooperation at administrative level among the EEAS, the Commission and Parliament, the Commission-led network against disinformation, Parliament's administrative taskforce against disinformation, and the ongoing cooperation with NATO, the G7, civil society and private industry when it comes to cooperating on intelligence, analysis, the sharing of best practices and raising awareness about foreign information manipulation and interference; welcomes the European Court of Auditors (ECA) Special Report 09/2021 entitled 'Disinformation affecting the EU: tackled but not tamed'; calls on the EEAS and the Commission to publish a detailed timeline for the implementation of the ECA's recommendations;

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

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

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

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

24. Stresses the importance of broadly distributed, competitive, pluralistic media, independent journalists, fact-checkers and researchers, and a strong public service media 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 and the European Endowment for Democracy; deeply regrets that the European Digital Media Observatory does not cover the Baltic states; welcomes, too, initiatives aiming at establishing journalism and fact-checking trustworthiness indicators that are easy to recognise, such as that initiated by Reporters

Without Borders; calls on the Commission to counter monopolistic mass-media ownership;

25. 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;

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

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

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

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

30. 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 comprehensive training modules 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;

31. Underlines the need to raise awareness about foreign interference in all layers of society; welcomes the initiatives taken by the EEAS, the Commission and Parliament's

administration, such as training and awareness-raising events for journalists, teachers, influencers, students, senior citizens and visitors, both offline and online, in Brussels and across the Member States, and recommends that they be further developed;

32. Calls on the Member States, the EU administration and civil society organisations to share best practices for media and information literacy training and awareness-raising, as requested in the Audiovisual Media Services Directive [1] ; calls on the Commission to organise these exchanges in cooperation with the Media Literacy Expert Group; underlines that the revised directive needs to be rapidly and properly implemented by the Member States;

33. Urges the EU institutions to draw up a Code of Ethics to guide public authorities and political representatives in the use of social media platforms and networks; considers it necessary to encourage responsible use of such platforms and networks to combat manipulation and misinformation originating in the public sphere;

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

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

36. Recognises that gendered disinformation attacks and campaigns are often used as part of a broader political strategy to undermine equal participation in democratic processes, especially for women and LGBTIQ+ people; stresses that disinformation about LGBTIQ+ people fuels hate, both online and offline, and threatens lives; calls for research into online disinformation to be carried out with an intersectional lens and for oversight of the changes platforms are making to respond to gendered disinformation campaigns online; calls for increased attention to be paid to gender-based disinformation through the creation of early warning systems through which gendered disinformation campaigns can be reported and identified;

37. Calls on the Commission to put forward an overarching media and information literacy strategy with a special focus on combating information manipulation;

---

[1] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (OJ L 95, 15.4.2010, p. 1).

38. Welcomes the establishment of the expert group on tackling disinformation and promoting digital literacy through education and training, which will focus on critical thinking, teacher training, pre-bunking, debunking and fact-checking efforts, and student engagement, among other tasks; calls on the Commission to share the results of the work of this expert group and to implement its conclusions;

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

40. Calls on Member States to ensure effective public communication campaigns in relation to the COVID-19 pandemic in order to disseminate accurate and timely information to counteract misinformation, particularly in relation to vaccines;

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

42. Is deeply concerned about attacks, harassment, violence and threats against journalists, human rights defenders and other persons exposing foreign interference, which may also undermine their independence; calls on the Commission to swiftly submit concrete and ambitious proposals on the safety of all these persons, including an anti-strategic lawsuit against public participation (SLAPP) instrument and economic, legal and diplomatic support, as announced under the European Democracy Action Plan; welcomes, in this regard, Commission Recommendation (EU) 2021/1534 of 16 September 2021 on ensuring the protection, safety and empowerment of journalists and other media professionals in the European Union[1]; calls on the Member States to effectively protect journalists and other media professionals by means of legislative and non-legislative tools;

43. 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

[1] OJ L 331, 20.9.2021, p. 8.

that local knowledge is often needed to identify and implement adequate countermeasures;

44. Calls on the Commission and the Member States to establish communication channels and set up platforms where companies, NGOs and individuals, including members of diasporas, can report instances in which they fall victim to information manipulation or interference; calls on the Member States to support those who are victims of attacks and those who are aware of such attacks or are being put under pressure;

Foreign interference using online platforms

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

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

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

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

49. Calls on the Commission to fully take into account the Council of Europe's guidance note on best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation, adopted in June 2021;

50. Calls for full and effective implementation of the General Data Protection Regulation,[1] which limits the amount of data platforms can store about users and how long this data can be used, especially for platforms and applications using very private and/or sensitive data, such as messaging, health, finance and dating apps and small discussion groups; calls for gatekeeper platforms to refrain from combining personal data with personal data from other services offered by the gatekeeper or with personal data from third-party services, to make it equally easy to disagree as to agree to the storage and sharing of data and to allow users to choose whether to be targeted with other personalised advertising online; welcomes all efforts to ban micro-targeting techniques for political advertising, particularly but not limited to those based on sensitive personal data, such as ethnic origin, religious beliefs or sexual orientation, and asks the Commission to consider extending a ban on micro-targeting to issue-based advertising;

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

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

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

54. Calls for clear and readable labelling of deepfakes, both for platform users and in content metadata, to improve their traceability for researchers and fact-checkers; in this respect, welcomes the initiatives aimed at improving content authenticity and traceability, such as the development of watermarks and authenticity standards, and the introduction of global standards;

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, p. 1).

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

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

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

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

59. Calls for legislative rules to ensure transparency vis-à-vis users and the general public, such as obligating platforms to set up public and easily searchable archives of online advertisements, including who they are targeted at and who paid for them, and moderated and deleted content, establish self-regulatory measures and give comprehensive and meaningful access to information about the design, use and impact of algorithms to national competent authorities, vetted researchers affiliated with academic institutions, the media, civil society organisations and international organisations representing the public interest; believes that the metrics of these libraries should be harmonised to allow for cross-platform analysis and reduce the administrative burden for platforms;

60. Calls for an end to business models that rely on encouraging people to stay on platforms longer by feeding them engaging content; calls on legislative decision-makers and platforms to ensure, through the use of human moderators and a third party auditor, that algorithms do not promote illegal, extremist, discriminatory or radicalising content, but rather offer users a plurality of perspectives and prioritise and promote facts and

science-based content, in particular on important social issues such as public health and climate change; considers that engagement-based and addictive ranking systems pose a systemic threat to our society; calls on the Commission to address the current issue of price incentives, where highly targeted ads with divisive content often have much lower prices for the same amount of views than less-targeted ads with socially integrative content;

61. Calls for algorithms to be modified in order to stop boosting content originating from inauthentic accounts and channels that artificially drive the spread of harmful foreign information manipulation; calls for algorithms to be modified so that they do not push divisive and anger-inducing content; stresses the need for the EU to put in place measures to legally require social media companies to prevent the amplification of disinformation once detected to the greatest extent possible, and that there must be consequences for platforms if they do not comply with the requirement to take down disinformation;

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

63. Is alarmed by the average of EUR 65 million in ad revenue that flows each year to approximately 1 400 disinformation websites targeting EU citizens[1]; underlines that online advertisements, sometimes even by public institutions, end up on, and therefore finance, malicious websites promoting hate speech and disinformation, without the consent or even knowledge of the advertisers concerned; notes that five companies, including Google Ads, pay 97 % of these ad revenues and are responsible for selecting the publishers' websites listed in their inventory, and so have the power to determine which content is monetised and which not; considers it unacceptable that the algorithms which distribute the advertising funds are a complete black box for the public; calls on the Commission to make use of the tools of competition policy and anti-trust law to ensure a functional market and break up this monopoly; calls on these actors to prevent disinformation websites from being funded by their ad services; congratulates organisations dedicated to raising awareness about this concerning issue; underlines that advertisers should have the right to know and decide where their advertisements are placed and which broker has processed their data; calls for the establishment of a mediation process that allows advertisers to be refunded when ads are placed on websites that promote disinformation;

64. Underlines that the updated Code of Practice on Disinformation, the Digital Services Act, the Digital Markets Act and other measures linked to the European Democracy Action Plan will require an effective overview, assessment and sanctions mechanism after their adoption, in order to evaluate their implementation at national and EU level on a regular basis and identify and remedy loopholes without delay, and to sanction the misapplication of and failure to apply the commitments; calls, in this respect, for strong and resourceful digital service coordinators in each Member State, as well as sufficient resources to enable the enforcement arm of the Commission to execute the tasks it is

[1] https://disinformationindex.org/wp-content/uploads/2020/03/GDI_Adtech_EU.pdf

assigned under the Digital Services Act; stresses, furthermore, the importance of ensuring that online platforms are subject to independent audits certified by the Commission; notes that auditors cannot be funded by individual platforms in order to ensure their independence;

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

66. Is deeply concerned by the lack of transparency in the revision of the Code of Practice on Disinformation, as the discussion has remained largely the preserve of the private sector and the Commission; regrets that the European Parliament, in particular the INGE Special Committee, and some other key stakeholders were not properly consulted during the drafting of the review of the Code of Practice;

67. Deplores the continued self-regulatory nature of the Code of Practice, since self-regulation is insufficient when it comes to protecting the public from interference and manipulation attempts; is worried that the updated Code of Practice on Disinformation may not be able to provide an answer to the challenges ahead; is concerned by the strong reliance of the guidance to strengthen the Code of Practice on the Commission's Digital Services Act proposal; calls for swift action to ensure that the Code of Practice incorporates binding commitments for platforms to ensure the EU's readiness before the next local, regional, national and European elections;

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

69. Stresses the need for the code to be able to function as an effective tool until the entry into force of the Digital Services Act (DSA); believes that the code should frontload some of the obligations of the DSA and oblige signatories to implement a number of DSA provisions with regard to data access for researchers and regulators, and advertising transparency, including algorithmic and recommender system transparency; urges signatories to have their compliance with these obligations audited by an independent auditor and calls for these audit reports to be published;

70. Deplores the lack of transparency in the process of monitoring compliance with the code, as well as the timing of the revision of the code, which will be finalised before the conclusion of the INGE Special Committee; notes that at the very least, meeting agendas, concluding notes and attendance lists should be made publicly available; urges

signatories to testify in Parliament about their commitments regarding the code and the way they have and will implement these commitments;

71. Believes that independent media regulators, such as the European Regulators Group for Audiovisual Media Services, could have a crucial role to play in monitoring and enforcing the code;

72. Welcomes the proposal to establish a taskforce set out in the Commission's guidance on strengthening the code; insists that the Commission invite representatives of Parliament, national regulators and other stakeholders, including civil society and the research community, to be part of this taskforce;

Critical infrastructure and strategic sectors

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

74. Recommends that Member States maintain the prerogative to identify critical entities, but that coordination at EU level is necessary to:

(a) strengthen the connection and communication channels used by multiple actors, including for the overall security of EU missions and operations;

(b) support the competent authorities in Member States through the Critical Entities Resilience Group, ensuring a diverse participation of stakeholders, and notably the effective involvement of small and medium-sized enterprises (SMEs), civil society organisations and trade unions;

(c) promote the exchange of best practices not only among Member States but also at regional and local level, including with the Western Balkans, and among owners and operators of critical infrastructure, including through interagency communication, in order to identify concerning developments at an early stage and develop adequate countermeasures;

(d) implement a common strategy for responding to cyberattacks on critical infrastructure;

75. Recommends that the list of critical entities could be extended to include digital election infrastructure and education systems given their crucial importance in guaranteeing the long-term functioning and stability of the EU and its Member States, and that flexibility should be allowed when deciding on the addition to the list of new strategic sectors to be protected;

76. 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 that there is a lack of democratic oversight over the private sector; calls for more democratic oversight of platforms, including appropriate access to data and algorithms for competent authorities;

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

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

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

80. Calls for further development of European networks of data infrastructure and service providers with European security standards, such as GAIA-X, which is an important step in building viable alternatives to existing service providers and towards an open, transparent and secure digital economy; underlines the need to strengthen SMEs and

avoid cartelisation of the cloud market; recalls that data centres are critical infrastructures; is concerned about the influence of third countries and their companies on the development of GAIA-X;

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

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

Foreign interference during electoral processes

83. Calls for the protection of the entire electoral process to be established as a top EU and national security issue, since free and fair elections are at the heart of the democratic process; calls on the Commission to develop a better response framework to counter foreign interference in electoral processes, which among other measures should consist of direct communication channels with citizens;

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

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

86. Highlights the utmost importance of election observation missions in providing relevant information and issuing specific recommendations to make the electoral system more resilient and to help counter foreign interference in electoral processes; calls for electoral processes to be improved and strengthened, electoral observation missions being a key instrument in the fight against the increasing use of unfair and rigged

electoral processes by illiberal regimes seeking to appear democratic; stresses in this connection the need to reassess and update the tools and methods used in international election observation in order to address new trends and threats, including the fight against fake electoral observers, the exchange of best practices with like-minded partners, and closer collaboration with relevant international organisations such as the Organization for Security and Co-operation in Europe (OSCE) and the Council of Europe, and all relevant actors in the framework of the Declaration of Principles for International Election Observation and the Code of Conduct for International Election Observers; stresses that the participation of MEPs in unauthorised election observation missions undermines the credibility and reputation of the European Parliament; welcomes and recommends the full enforcement of the Democracy Support and Election Coordination Group procedure for 'cases of individual unofficial election observation by Members of the European Parliament' (adopted on 13 December 2018) which allows for the exclusion of MEPs from Parliament's official election observation delegations for the duration of the mandate;

Covert funding of political activities by foreign donors

87. Stresses that, while there is still a need for a better understanding of the effects of covert financing of political activities on, for example, anti-democratic tendencies in Europe, foreign funding of political activities through covert operations nevertheless 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; stresses that it should therefore be made illegal in all Member States to engage in any covert activity financed by foreign actors that aims to influence the process of European or national politics; notes in this respect that countries such as Australia have implemented laws that ban foreign interference in politics;

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

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

    (a) in-kind contributions from foreign actors to political parties, foundations, people who hold public office or elected officials, including financial loans from any legal or physical persons based outside the EU and the European Economic Area (EEA) (except European voters), anonymous donations above a certain threshold, and the lack of spending limits for political campaigns which allows for influence through large donations; political individuals, actors or parties who have been offered and/or accepted a financial or in-kind contribution by a foreign actor must be obliged to report it to the competent authorities and this information should be reported in turn at EU level to allow for EU-wide monitoring;

(b) straw donors with domestic citizenship[1]: 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; donations from within the EU that exceed a certain minimum threshold should be registered in an official and public register and linked to a natural person, and a ceiling should be set for donations from private and legal persons (and subsidies) to political parties;

(c) shell companies and domestic subsidiaries of foreign parent companies[2]: shell companies should be prohibited and more robust requirements established in order to reveal the origins of funding through parent companies; funding and donations to political parties beyond a certain threshold must be registered in a public and central register with an official name and address that can be linked to an existing person, and Member States should collect that information; calls on the Commission to ensure that authorities in Member States have the right to investigate the origins of funding to verify the information from domestic subsidiaries and to address the lack of sufficient data in national registers, especially in situations in which a network of shell companies is used;

(d) non-profit organisations and third parties[3], coordinated by foreign actors and created with a view to influencing electoral processes: more uniform rules and transparency should be considered across the EU for organisations aiming to finance political activities when seeking to directly influence electoral processes such as elections and referendum campaigns; such rules should not prevent non-profit organisations and third parties from receiving funding for issue campaigns; rules ensuring the transparency of funding or donations must also apply to political foundations;

(e) online political advertisements are not subject to the rules on TV, radio and print advertising and are usually not regulated at EU level: there is therefore a need to prohibit advertisements bought by actors coming from outside the EU and the EEA and guarantee complete transparency with regard to the purchasing of online political advertisements by actors from within the EU; underlines the need to ensure much greater transparency and democratic accountability as to the use of algorithms; welcomes the announcement of a new legislative proposal on the transparency of sponsored political content by the Commission, as proposed under the European Democracy Action Plan, which should aim to prevent a patchwork of 27 different national bodies of legislations on online political advertising and will guarantee that EU parties are able to campaign online ahead of the European elections while limiting the risk of foreign interference and exploring which of the rules that political parties within single Member States and major social media platforms have voluntarily adopted can be made rules for everyone in the EU; calls on the Member States to update their national political advertising rules, which have not kept pace with the steady evolution towards the digital medium as

---

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

2 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.

3 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.

the primary mode of political communication; calls on the Commission to propose how to democratically define issue-based political advertising to end a situation where private for-profit platforms decide what is issue-based and what is not;

(f) monitoring of election spending through independent auditors should be implemented and information on spending and donations made available to independent auditors in a timely manner, mitigating risks such as conflicts of interest and lobbying in relation to political finance; in establishing proactive disclosure, institutions responsible for finance regulations should have a clear mandate, and the ability, resources and legal power to conduct investigations and refer cases for prosecution;

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

91. Undertakes to ensure that all non-profit organisations, think tanks, institutes and NGOs that are given input in the course of parliamentary work into the development of EU policy or any consultative role in the lawmaking process are fully transparent, independent and free from conflicts of interest in terms of their funding and ownership;

92. Welcomes the ongoing revision of Regulation (EU, Euratom) No 1141/2014 on the statute and funding of European political parties and foundations; supports all efforts to achieve a greater level of transparency in the financing of the activities of European political parties and foundations, in particular ahead of the European elections of 2024, including a ban on all donations from outside the EU and anonymous sources, with the exception of the diaspora from EU Member States, and on donations from outside the EU that cannot be documented through either contracts, service agreements or fees associated with affiliation to European political parties, while allowing membership fees from national member parties outside the EU and EEA to European political parties; urges European and national political parties to commit to fighting foreign interference and combating the spread of disinformation by signing a charter containing specific commitments in this respect;

93. Stresses that implementation of many of the Council of Europe GRECO and Venice Commission recommendations would strengthen the immunity of the political system of Member States and the Union as a whole from foreign financial influence;

Cybersecurity and resilience against cyberattacks

94. Urges the EU institutions and the Member States to rapidly increase investments in the EU's strategic cyber capacities and capabilities to detect, expose and tackle foreign interference, such as AI, secured communication, and data and cloud infrastructure, in order to improve the EU's cybersecurity, while ensuring respect for fundamental rights; calls on the Commission to also invest more in increasing the EU's digital knowledge and technical expertise so as to better understand the digital systems used across the EU; calls on the Commission to allocate additional resources, human, material and financial, to cyber threat analysis capabilities, namely the EEAS's INTCEN, and the cybersecurity of the EU institutions, bodies and agencies, namely ENISA and the Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU), and the Member States; regrets the lack of cooperation and harmonisation on cybersecurity matters among Member States;

95. 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[1] (NIS2); recommends that the final outcome of the ongoing work on the proposal address the flaws of the 2016NIS Directive, notably by strengthening security requirements, broadening its scope, creating a framework for European cooperation and information sharing, strengthening Member States' cybersecurity capabilities, developing public-private cooperation, introducing stricter enforcement requirements and making cybersecurity a responsibility at the highest level of management in European entities that are vital for our society; emphasises the importance of reaching a high common level of cybersecurity across all Member States so as to limit weak points in joint EU cybersecurity; underlines the crucial need to ensure the resilience of information systems and welcomes in this regard the Cyber Crisis Liaison Organisation Network (CyCLONe); encourages the further promotion of the OSCE confidence-building measures for cyberspace;

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

97. Stresses that cybercrime has no borders and urges the EU to step up its international efforts to tackle it effectively; points out that the EU should take the lead in the development of an International Treaty on Cybersecurity that lays down international norms on cybersecurity to fight cybercrime;

98. Insists on the need for the EU, NATO and like-minded international partners to step up their cybersecurity assistance to Ukraine; welcomes the initial deployment of experts from the PESCO-funded Cyber Rapid Response Team and calls for full use of the EU

[1] 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).

cyber sanctions regime against the individuals, entities and bodies responsible for or involved in the various cyberattacks targeting Ukraine;

99. Welcomes the announcement of the creation of a Cyber Resilience Act that would complement a European Cyber Defence Policy, as cyber and defence are closely related; calls for more investments in European cyber defence capabilities and coordination; recommends that the cyber capability-building of our partners be fostered through EU training missions or civilian cyber missions; underlines the need to harmonise and standardise cyber-related training and calls for structural EU funding in that area;

100. Condemns the massive-scale and illicit use of the NSO Group's Pegasus surveillance software by state entities, such as Morocco, Saudi Arabia, Hungary, Poland, Bahrain, the United Arab Emirates and Azerbaijan, against journalists, human rights defenders and politicians; recalls that Pegasus is only one of the many examples of a program that is abused by state entities for illicit mass surveillance purposes against innocent citizens; also condemns other state spying operations targeted against European politicians; urges the Commission to draw up a list of illicit surveillance software and to continuously update this list; calls for the EU and Member States to use this list in order to ensure full human rights due diligence and proper vetting of exports of European surveillance technology and technical assistance and imports to Member States which pose a clear risk to the rule of law; calls, in addition, for the establishment of an EU Citizens' Lab, similar to that established in Canada, comprising journalists, human rights experts and reverse malware engineering experts, which would work to discover and expose the unlawful use of software for illicit surveillance purposes;

101. Calls for the EU to adopt a robust regulatory framework in this field, both within the EU and at international level; welcomes, in this regard, the decision of the US Commerce Department's Bureau of Industry and Security to blacklist NSO Group Technologies, thereby prohibiting the company from receiving American technologies;

102. Expresses its concern that the EU is cooperating on judicial and law enforcement matters with third countries that have been involved with NSO Group and that have been using the Pegasus spyware to spy on EU citizens; calls for additional safeguards and enhanced democratic scrutiny of such cooperation;

103. Calls on the Commission to review EU investments in NSO Group Technologies and to adopt targeted measures against foreign states using software to spy on EU citizens or persons benefiting from refugee status in EU countries;

104. 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, 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;

105. Points out the urgent need to reinforce the legislative framework so as to hold accountable those who distribute, use and abuse such software for illicit and unauthorised purposes; refers, in particular, to the sanctions imposed on 21 June 2021 on Alexander Shatrov, CEO of a Belarusian company producing facial recognition

software used by an authoritarian regime, for example to identify political opposition protesters; calls on the Commission to prevent any use or funding in the EU of illegal surveillance technologies; calls for the EU and Member States to engage with third-country governments to end repressive cybersecurity and counter-terrorism practices and legislation, under enhanced democratic scrutiny; calls for an investigation by the competent EU authorities into the unlawful use of spyware in the EU and exports of such software from the EU, and for repercussions for Member States and associated countries, including those participating in EU programmes, which have bought and used such spyware and from which it has been exported to illegally target journalists, human rights defenders, lawyers and politicians;

106. Calls for an ambitious revision of the ePrivacy Directive[1] 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 directive, and without prejudice to Member States' responsibility to safeguard national security; highlights that public authorities should be obliged to disclose vulnerabilities they find in IT devices; calls for the EU and Member States to further coordinate their actions based on the Directive on Attacks against Information Systems[2] in order to ensure that illegal access to information systems and illegal interception are defined as criminal offences and met with appropriate sanctions; recalls that every breach of confidentiality for national security purposes must be carried out lawfully and for explicit and legitimate purposes in a democratic society, on the basis of strict necessity and proportionality, as required by the ECHR and the Court of Justice of the European Union;

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

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

108. Calls for a thorough and periodical review of all the services, networks, equipment and hardware of EU institutions, bodies, agencies, delegations, missions and operations in order to bolster their resilience to cybersecurity threats and exclude potentially dangerous programmes and devices, such as those developed by Kaspersky Lab; urges the EU institutions and the Member States to ensure proper guidance and secure tools for staff; emphasises the need to raise awareness of the use of secure services and networks within institutions and administrations, including while on mission; notes the

---

1 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ L 201, 31.7.2002, p. 37).

2 Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.8.2013, p. 8).

trust and security advantages of open-source-based network operating systems, which are widely used by allied military and government agencies;

109. Stresses the importance of efficient, timely and close coordination between different EU institutions, bodies and agencies specialised in cybersecurity, such as CERT-EU, alongside the full development of its operational capabilities, as well as ENISA and the upcoming Joint Cyber Unit, which will ensure a coordinated response to large-scale cybersecurity threats in the EU; welcomes the ongoing structured cooperation between CERT-EU and ENISA; welcomes, too, the establishment of the EU cyber intelligence working group within EU INTCEN with a view to advancing strategic intelligence cooperation; appreciates the recent initiatives taken by the Secretaries-General of the EU institutions to develop common information and cybersecurity rules;

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

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

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

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

114. 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 strengthen its monitoring, inter alia through the establishment of a central repository and incident tracking tool, and to develop a shared toolbox to be activated in the event of an RAS alert;

115. Calls for mandatory transparency rules for trips offered by foreign countries and entities to officials of the EU institutions, including MEPs, APAs and group advisors, as well as for national officials, including but not limited to: the name of paying agents, the cost of trips and the stated motives; recalls that such organised trips cannot be considered official Parliament delegations and calls for strict sanctions should this not be respected; stresses that informal friendship groups can undermine the work of the official bodies of Parliament, as well as its reputation and the coherence of its actions; urges Parliament's governing bodies to increase the transparency and accountability of these groups, to enforce current rules and to take the necessary measures when these friendship groups are misused by third countries; asks the Quaestors to develop and maintain an accessible and up-to-date register of friendship groups and declarations;

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

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

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

118. 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; calls for effective cooperation on this matter among all EU institutions; considers Australia's Foreign Influence Transparency Scheme to be a good practice to follow;

119. 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;

120. 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;

121. Strongly condemns the Kremlin's efforts to instrumentalise minorities in EU Member States by implementing so-called compatriot policies, particularly in the Baltic states and the Eastern Neighbourhood countries, as part of the geopolitical strategy of Putin's regime, whose aim is to divide societies in the EU, alongside the implementation of the concept of the 'Russian world', aimed at justifying expansionist actions by the regime; notes that many Russian 'private foundations', 'private enterprises', 'media organisations' and 'NGOs' are either state-owned or have hidden ties with the Russian state; stresses that it is of the utmost importance when engaging in dialogue with Russian civil society to differentiate between those organisations which stay clear of Russian governmental influence and those that have links to the Kremlin; recalls that there is also evidence of Russian interference and manipulation in many other Western liberal democracies, as well as active support for extremist forces and radical-minded entities in order to promote the destabilisation of the Union; notes that the Kremlin makes broad use of culture, including popular music, audiovisual content and literature, as part of its disinformation ecosystem; deplores Russia's attempts not to fully recognise the history of Soviet crimes and instead to introduce a new Russian narrative;

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

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

124. Stresses the need for the EU and its Member States to enhance support to Eastern Partnership countries, in particular through cooperation on building state and societal resilience to disinformation and Russian state propaganda, in order to counter the strategic weakening and fragmentation of their societies and institutions;

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

126. Is worried about the number of European universities, schools and cultural centres engaged in partnerships with Chinese entities, including Confucius Institutes, which enable the theft of scientific knowledge and the exercise of strict control over all topics related to China in the field of research and teaching, thus constituting a violation of the constitutional protection of academic freedom and autonomy, and over the choices of cultural activities related to China; is worried that such actions might lead to a loss of knowledge on China-related issues, depriving the EU of the necessary competences; is concerned, for example, by the sponsoring, in 2014, of the China Library of the College of Europe by the State Council Information Office of the Chinese Government[1]; is deeply concerned about China's attempts to pressure and censor, for example, the museum of Nantes in relation to the exhibition on Genghis Kahn initially planned for 2020[2]; invites the Commission to facilitate the exchange of good practices among Member States in order to tackle foreign interference in the cultural and educational sectors;

127. Is concerned about cases of concealed financing of research conducted in Europe, including China's attempts to poach talent through the Thousand Talents Plan and the Confucius Institute Scholarships, and the deliberate blending of military and civil scientific projects through China's civil-military fusion strategy; highlights attempts by Chinese higher education institutions to sign memorandums of understanding with partner institutions in Europe which contain clauses that perpetuate Chinese propaganda or encourage support for Chinese Communist Party standpoints or political initiatives, such as the Belt and Road Initiative, thereby bypassing and undermining official positions taken by the governments of the respective countries; asks cultural, academic and non-governmental institutions to improve transparency as regards China's influence and calls on them to publicise any exchanges and engagements with the Chinese Government and related organisations;

128. Condemns the decision taken by the Hungarian Government to open a Fudan University branch while, at the same time, closing the Central European University in Budapest; is concerned about the increasing financial dependence of European universities on China and other foreign states, given the risk of sensitive data, technologies and research outcomes flowing to foreign states and the implications this dependence could have for academic freedom; stresses the importance of academic freedom to address disinformation and influence operations; encourages these institutions to conduct detailed vulnerability assessments before entering into new partnerships with foreign partners; stresses that academic staff should be trained to report covert funding or

[1] https://www.coleurope.eu/events/official-inauguration-china-library
[2] https://www.chateaunantes.fr/expositions/fils-du-ciel-et-des-steppes/

influence through a dedicated hotline and that those coming forward should always receive whistleblower protection; calls on the Commission and Member States to ensure that funding for research of geopolitical concern at European universities comes from European sources; calls on the Commission to propose legislation on increasing the transparency of the foreign financing of universities, as well as NGOs and think tanks, such as through mandatory donation declarations, due diligence for their funding streams and the disclosure of funding, in-kind contributions and subsidies from foreign parties; calls on Member State authorities to adopt effective rules on foreign funding for higher education institutions, including strict ceilings and reporting requirements;

129. Underlines that similar risks to security and intellectual property theft exist in the private sector, where employees might have access to key technologies and trade secrets; calls on the Commission and Member States to encourage both academic institutions and the private sector to set up comprehensive security and compliance programmes, including specific security reviews for new contracts; notes that heightened limitations on systems and network access, as well as security clearance, may be warranted for some of the professors or employees working on critical research and products;

130. Notes that the revised Blue Card Directive[1], which makes it easier for skilled non-EU migrants to come to the EU, enables Chinese and Russian companies established in Europe, for example, to bring over skilled migrants from their respective countries; points out that this could make it more difficult for Member States to exercise control over the influx of these citizens, which might lead to risks of foreign interference;

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

132. 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 agents and spies; recalls that many universities have decided to terminate their cooperation with Confucius Institutes because of the risks of Chinese espionage and interference, as did the universities of Dusseldorf in 2016, Brussels (VUB and ULB) in 2019, and Hamburg in 2020, and all universities in Sweden; calls for more universities to reflect on their current cooperation to ensure that it does not affect their academic freedom; calls on Member States to closely monitor teaching, research and other activities within the Confucius Institutes and, where alleged espionage or interference is substantiated by clear evidence, take enforcement action to safeguard European

[1] Directive (EU) 2021/1883 of the European Parliament and of the Council of 20 October 2021 on the conditions of entry and residence of third-country nationals for the purpose of highly qualified employment, and repealing Council Directive 2009/50/EC (OJ L 382, 28.10.2021, p. 1).

economic and political sovereignty, including through the denial of funding or the revocation of the licences of associated institutes;

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

134. Calls on the EEAS to produce a study into the prevalence and influence of malicious state actors in European think tanks, universities, religious organisations and media institutions; calls on all EU institutions and Member States to collaborate with and engage in systematic dialogue with stakeholders and experts in order to accurately map and monitor foreign influence in the cultural, academic and religious spheres; calls for greater content sharing among European national broadcasters, including those in neighbouring countries;

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

Deterrence, attribution and collective countermeasures, including sanctions

136. 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[1] and the EU Global Human Rights Sanctions Regime[2] (EU Magnitsky Act), adopted on 17 May 2019 and 7 December 2020 respectively, have demonstrated added value in providing the EU with valuable deterrence tools; calls on the Commission to put forward a legislative proposal to adopt a new thematic sanctions regime to address serious acts of corruption; recalls that the cyberattack and human rights sanctions regimes have been used twice, in 2020 and 2021 respectively; urges that the cyber sanctions regime be made permanent and calls on Member States to share all evidence and intelligence gathered in order to feed into the establishment of cyber sanction lists;

---

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

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

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

138. 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, and must be transparent as regards the grounds on which the decision to implement sanctions is taken; stresses the need for greater clarity at EU level regarding the scope and impact of sanctions against associated persons, such as EU nationals and companies;

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

140. 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';

141. 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[1];

142. Underlines that, in order to reinforce their impact, sanctions should be imposed collectively, based, where possible, on coordination with like-minded partners, possibly involving international organisations and formalised in an international agreement, considering also other types of reactions to the attacks; notes that candidate and potential candidate countries should also adopt these sanctions in order to align with the EU's CFSP; notes the important work done by NATO in the area of hybrid threats and recalls in this respect the communiqué of the NATO meeting of 14 June 2021, where it was reaffirmed that a decision as to when a cyberattack would lead to the invocation of Article 5 of the NATO Treaty would be taken by the North Atlantic Council on a case-by-case basis, and that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack[2]; stresses that the EU and NATO should adopt a more forward-looking and strategic approach towards hybrid threats focused on the motives and objectives of adversaries, and should clarify in which instances the EU is better equipped to deal with a threat, as well as the comparative advantages of their capabilities; recalls that several EU Member States are not members of NATO, but nevertheless cooperate with NATO, for instance through its Partnership for Peace (PfP) programme and Partnership Interoperability Initiative (PII), and therefore underlines that any EU-NATO cooperation must be without prejudice to the security and defence policy of the non-NATO EU Member States, including those which have neutrality policies in place; stresses the importance of mutual assistance and solidarity in line with Article 42(7) TEU and Article 222 TFEU and calls for the EU to draw up concrete scenarios for the activation of these articles in the event of a hypothetical cyberattack; calls on the EU and all Member States to link the issue with the other aspects of their relations with the states behind interference and disinformation campaigns, in particular Russia and China;

Global cooperation and multilateralism

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

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

145. Considers that, on the basis of common situational awareness, like-minded partners should exchange best practices and identify common responses to global, but also

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

shared domestic, challenges, including collective sanctions, the protection of human rights and democratic standards; calls for the EU to lead the debate on the legal implications of foreign interference, to promote common international definitions and attribution rules and to develop an international framework for responses to interference in elections in order to establish a Global Code of Practice for Free and Resilient Democratic Processes;

146. Calls for the EU and its Member States to consider the right international formats to allow for such a partnership and cooperation between like-minded partners; calls for the EU and its Member States to initiate a process at UN level to adopt a global convention to promote and defend democracy that establishes a common definition of foreign interference; calls for the EU to propose a global democracy defence toolkit, to be included in the convention, containing joint actions and sanctions to counter foreign interference;

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

148. 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;

149. Underlines that global cooperation should be based on common values reflected in common projects, involving international organisations such as the OSCE and UNESCO, and setting up democratic capacity building and sustainable peace and security in countries facing similar foreign interference threats; calls for the EU to establish a European Democratic Media Fund to support independent journalism in (potential) enlargement and European neighbourhood countries and in candidate and potential candidate countries; highlights the practical needs, such as obtaining technical work equipment, regularly voiced by independent journalists from neighbouring countries;

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

151. Stresses the importance of providing a clear perspective for candidate and potential candidate countries and of supporting partner and neighbouring countries, such as those in the Western Balkans and the Eastern and Southern Neighbourhoods of the EU, since

countries such as Russia, Turkey and China are trying to use these countries as an information manipulation and hybrid warfare laboratory, aimed at undermining the EU; believes that the US is an important partner in countering foreign interference, disinformation campaigns and hybrid threats in those regions; is worried in particular by the role played by Serbia and Hungary in widely disseminating disinformation to surrounding countries; underlines that the EU should support and engage with these countries, as provided for in the NDICI Regulation[1]; considers that its actions can take the form of promoting the EU's added value and positive impact in the region, financing projects aimed at ensuring media freedom, strengthening civil society and the rule of law, and enhancing cooperation on media, digital and information literacy, while respecting the sovereignty of such countries; calls for increased EEAS capacity in this regard;

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

153. Calls for Parliament to actively promote an EU narrative, to play a leading role in promoting the exchange of information and to discuss best practices with partner parliaments across the globe, using its vast network of interparliamentary delegations, as well as the democracy initiatives and support activities coordinated by its Democracy Support and Election Coordination Group; underlines the importance of close cooperation with parliamentarians from third countries through tailor-made projects supporting a European perspective for candidate and potential candidate countries;

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

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

156. Calls for the creation of a permanent institutional arrangement in the European Parliament dedicated to the follow-up of these recommendations, in order to address

[1] Regulation (EU) 2021/947 of the European Parliament and of the Council of 9 June 2021 establishing the Neighbourhood, Development and International Cooperation Instrument – Global Europe, amending and repealing Decision No 466/2014/EU of the European Parliament and of the Council and repealing Regulation (EU) 2017/1601 of the European Parliament and of the Council and Council Regulation (EC, Euratom) No 480/2009 (OJ L 209, 14.6.2021, p. 1).

foreign interference and disinformation in the EU in a systematic way beyond the current mandate of the INGE Special Committee; calls for an improved institutionalised exchange between the Commission, the EEAS and Parliament through this body;

157. 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.

ING2

“Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation, and the Strengthening of Integrity, Transparency and Accountability in the European Parliament”

EPP GROUP MEMBERS OF THE EUROPEAN PARLIAMENT'S SPECIAL COMMITTEE (ING2)

Javier ZARZALEJOS
First Vice-Chair

Vladimír BILČÍK
Coordinator

Sandra KALNIETE
Member, Rapporteur

David LEGA
Vice-Coordinator

Ioan-Rareş BOGDAN
Member

Andrey KOVATCHEV
Member

Janusz LEWANDOWSKI
Member

Benoît LUTGEN
Member

Lukas MANDL
Member

Sabine VERHEYEN
Member

Salvatore DE MEO
Substitute

Geoffroy DIDIER
Substitute

Sunčana GLAVAK
Substitute

Rasa JUKNEVIČIENĖ
Substitute

Paulo RANGEL
Substitute

Maria SPYRAKI
Substitute

Isabel WISELER-LIMA
Substitute

Tomáš ZDECHOVSKÝ
Substitute

FINAL REPORT ING2

TEXTS ADOPTED

P9_TA(2023)0219

Foreign interference in all democratic processes in the European Union, including disinformation

European Parliament resolution of 1 June 2023 on foreign interference in all democratic processes in the European Union, including disinformation (2022/2075(INI))

The European Parliament

- having regard to its decision of 10 March 2022 on setting up a special committee on foreign interference in all democratic processes in the European Union, including disinformation (INGE 2), and defining its responsibilities, numerical strength and term of offices[1] , and its decision of 14 February 2023 amending its aforementioned decision of 10 March, and adjusting its title and responsibilities[2],

- having regard to its resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation[3] (hereinafter the 'INGE 1 report'),

- having regard to the Commission's follow-up to Parliament's recommendations in its resolution of 9 March 2022,

- having regard to the Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security, approved by the Council on 21 March 2022 and endorsed by the European Council on 24 March 2022,

- having regard to its recommendation of 23 November 2022 to the Council, the Commission and the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy concerning the new EU strategy for enlargement[4],

- having regard to the Commission communication of 13 July 2022 entitled '2022 Rule of Law Report – The rule of law situation in the European Union' (COM(2022)0500),

- having regard to its resolution of 8 March 2022 on the shrinking space for civil society

[1] Texts adopted, P9_TA(2022)0070.
[2] Texts adopted, P9_TA(2023)0030.
[3] OJ C 347, 9.9.2022, p. 61.
[4] Texts adopted, P9_TA(2022)0406.

in Europe[1],

- having regard to its resolution of 15 December 2022 on suspicions of corruption from Qatar and the broader need for transparency and accountability in the European institutions[2],

- having regard to its resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third countries[3]

- having regard to its recommendation of 13 March 2019 to the Council and the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy concerning taking stock of the follow-up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda against it by third countries[4],

- having regard to its resolution of 20 October 2021 entitled 'Europe's Media in the Digital Decade: an Action Plan to Support Recovery and Transformation'[5],

- having regard to the Articles of Responsibility of States for Internationally Wrongful Acts,

- having regard to the Charter of Fundamental Rights of the European Union,

- having regard to the International Covenant on Civil and Political Rights, in particular Article 20 thereof,

- having regard to Regulation (EU) 2021/692 of the European Parliament and of the Council of 28 April 2021 establishing the Citizens, Equality, Rights and Values Programme and repealing Regulation (EU) No 1381/2013 of the European Parliament and of the Council and Council Regulation (EU) No 390/2014[6] ,

- having regard to the Commission proposal of 27 April 2022 for a directive of the European Parliament and of the Council on protecting persons who engage in public participation from manifestly unfounded or abusive court proceedings ('Strategic lawsuits against public participation') (COM(2022)0177),

- having regard to the Commission communication of 3 December 2020 on the European democracy action plan (COM(2020)0790),

- having regard to the proposal of 16 September 2022 for a regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU (COM(2022)0457),

- having regard to the final report of the Conference on the Future of Europe, and in

---

1 OJ C 347, 9.9.2022, p. 2.
2 Texts adopted, P9_TA(2022)0448.
3 OJ C 224, 27.6.2018, p. 58.
4 OJ C 23, 21.1.2021, p. 152.
5 OJ C 184, 5.5.2022, p. 71.
6 OJ L 156, 5.5.2021, p. 1.

particular proposals 27 and 37 thereof,

– having regard to the strengthened Code of Practice on Disinformation 2022,

– having regard to Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)[1] ,

– having regard to Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC[2] (CER Directive);

– having regard to the Commission proposal of 18 October 2022 for a Council recommendation on a coordinated approach by the Union to strengthen the resilience of critical infrastructure (COM(2022)0551),

– having regard to the Commission proposal of 25 November 2021 for a regulation of the European Parliament and of the Council on the transparency and targeting of political advertising (COM(2021)0731) and the amendments thereto, adopted by Parliament on 2 February 2023[3],

– having regard to the Commission proposal of 25 November 2021 for a regulation of the European Parliament and of the Council on the statute and funding of European political parties and European political foundations (COM(2021)0734),

– 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) (NIS2 Directive),

– having regard to European Court of Auditors (ECA) special report 05/2022 of 29 March 2022 entitled 'Cybersecurity of EU institutions, bodies and agencies – Level of preparedness overall not commensurate with the threats',

– having regard to the Commission proposal of 22 March 2022 for a regulation of the European Parliament and of the Council laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (COM(2022)0122),

– having regard to the interinstitutional agreement of 20 May 2021 between the European Parliament, the Council and the Commission on a mandatory transparency register[4],

– having regard to the US-EU Joint Statement of the Trade and Technology Council of 5 December 2022,

– having regard to the ECA Annual Report on EU agencies for the financial year 2021,

---

1 OJ L 277, 27.10.2022, p. 1.
2 OJ L 333, 27.12.2022, p. 164.
3 Texts adopted, P9_TA(2023)0027.
4 OJ L 207, 11.6.2021, p. 1.

– having regard to the European Code of Standards for Independent Fact-Checking Organisations, published by the European Fact-Checking Standards Network in August 2022,

– having regard to Rules 54 and 207 of its Rules of Procedure,

– having regard to the (mid-term) report of the Special Committee on foreign interference in all democratic processes in the European Union, including disinformation, and the strengthening of integrity, transparency and accountability in the European Parliament (ING2) (A9-0187/2023),

A. whereas Parliament adopted a resolution on 9 March 2022 laying down its recommendations based on the report of the first special committee on foreign interference in all democratic processes in the European Union, including disinformation; whereas among its recommendations, this report called for the adoption of a coordinated strategy against foreign interference; whereas the Commission produced a document following up on these recommendations, suggesting among other things that such a strategy de facto already exists in the form of various kinds of interinstitutional coordination;

B. whereas the European Parliament is the only directly elected body among the EU institutions and is at the forefront of EU political discussions on fighting foreign interference, information manipulation and hybrid threats in our democracies, including in the EU institutions; whereas recent events have highlighted that Parliament is a target of diverse and aggressive foreign interference campaigns;

C. whereas the President of the Commission announced in her September 2022 State of the Union address that a Defence of Democracy package would be presented by the Commission, scheduled for adoption in the second quarter of 2023; whereas this package would include a legislative proposal to protect democracies from third-country entities exercising activities in the EU that may affect public opinion and the democratic sphere, a review of actions under the European democracy action plan (EDAP) and measures to ensure secure and resilient elections, including, among others, cybersecurity measures in electoral processes;

D. whereas the Council of the European Union, the Commission and the European External Action Service co-led a joint exercise called 'EU Integrated Resolve 2022' aimed at testing the EU's response to hybrid campaigns;

E. whereas Russia's war of aggression against Ukraine started as a carefully planned and aggressively executed information war followed by a full-scale military invasion on 24 February 2022; whereas Russia uses an array of different methods of interference, embedded within a larger strategy to harm, confuse, frighten, weaken and divide the EU's Member States and its neighbourhood; whereas the United States and the United Kingdom led effective 'pre-bunking' communication campaigns prior to Russia's full-scale invasion of Ukraine, involving making unprecedented public use of available reliable intelligence to counter the Kremlin narrative and shed light on the lies of the Russian Government and related actors; whereas Russia had for years been carrying out disinformation campaigns, cyber-attacks, elite capture and attacks aimed at rewriting history in an attempt to prepare the groundwork for its invasion of Ukraine to underpin it;

F. whereas Parliament's services are expected to make significant efforts to follow up on the recommendations adopted on 9 March 2022, in particular when preparing the 2024 European elections; whereas Parliament's task force on disinformation has been tasked with coordinating the work of different European Parliament Directorates-General and cooperating with other EU institutions on a number of actions undertaken in particular in the following fields: situational awareness, resilience building, pre-bunking and contribution to a healthy information space, and mitigation;

G. whereas Parliament is proactively supporting parliamentary democracy in a number of non-EU countries, including through the actions of the Democracy and Election Support Group (DEG); whereas the EU's immediate neighbourhood is particularly important in this regard;

H. whereas EU accession countries are facing challenges stemming from malign foreign interference and disinformation campaigns; whereas past developments have shown that non-enlargement has a serious strategic cost; whereas the Western Balkans are an area of strategic and geopolitical competition and some of its countries are prone to destabilisation, threatening the security and stability of our continent; whereas third countries are exploiting these vulnerabilities, including through strategic investments and disinformation campaigns; whereas the stability, security and democratic resilience of the accession countries are inextricably linked to the EU's own security, stability and democratic resilience;

I. whereas the aim of those interference campaigns in the Western Balkans is to negatively influence the growing euro-Atlantic orientation and stability of individual countries, and so change the orientation of the region as a whole; whereas Russia is using its influence in Serbia in an attempt to destabilise and interfere in neighbouring sovereign states: in Bosnia via the Republika Srpska; in Montenegro via the country's pro-Serbian sentiments as well as the Serbian Orthodox Church; and in Kosovo by exploiting and inflaming existing disputes in the North of Kosovo; whereas Russia therefore still has notable influence in the Western Balkans, with the power to interfere in regional attempts at reconciliation, integration and reform towards democratisation;

J. whereas initiatives such as the EU-funded RADAR project, from the Trans European Policy Studies Association (TEPSA, a pan-European consortium of leading research institutes and universities), aims to raise citizens' awareness of disinformation and provide a public platform for debate, and the project has a special focus on youth in order to empower their voices, strengthen their engagement in civil society and improve their education on critical thinking and media literacy;

K. whereas a holistic approach, encompassing our societies as a whole, is needed when educating and training European citizens of all ages, including specific training for people of working age and in schools to detect and be resilient against prospective disinformation operations and information manipulation; whereas a strategy should be established to pre-emptively show internet users videos and content on the tactics behind disinformation, which have the potential to make them more aware and resilient to misinformation and disinformation and increase the resilience of vulnerable population groups; whereas public awareness and constant dialogue with media is critical in this regard; whereas the central feature of communication success against disinformation is trust in the communicating institutions;

L. whereas contemporary antisemitism takes many forms, including online hate speech and the (re-)emergence of new conspiracy theories, and whereas the EU has, within the framework of the EU strategy on combating antisemitism and fostering Jewish life (2021-2030), established its commitment to a future free from antisemitism in the EU and beyond;

M. whereas civil society organisations (CSOs) play an essential role as watchdogs, are key to building democratic resilience from within and protecting democracy, and support the combat against breaches of the rule of law while actively contributing to fostering the rule of law, democracy and fundamental rights on the ground; whereas, specifically, CSOs play an important part in detecting and countering foreign interference in democratic processes; whereas CSOs play a critical role in developing self-regulation, enabling the creation of industry standards to fight disinformation, in particular in fields where any state actions may create mistrust; whereas when the participation of citizens and civil society in democratic processes is further strengthened, then the democracy as a whole is better fortified against the risk of foreign interference;

N. whereas CSOs, think tanks, consulting agencies, foundations and companies themselves are not immune from experiencing such interference and, in some cases, may serve as the vehicle, tool or vector of influence from malicious actors, including third-country actors, directly sponsoring or instigating foreign interference and influencing policymakers; whereas transparency is key to ensure that these actors do not become and are not used as vessels for foreign interference and therefore clear rules for their influence must be observed and scrutinised; whereas some EU Member States have attempted to implement mechanisms to screen foreign governmental funding for CSOs, especially from Russia and China;

O. whereas the EU support of CSOs through the Citizens Equality Rights and Values programme (CERV), stepped up efforts to support civil society organisations, in particular the smaller, local ones facing particular constraints; whereas certain Member States, through the national recovery and resilience programmes, have provided funding for capacity-building for fact-checking and tackling disinformation;

P. whereas, in spite of certain available financial resources, including successful projects from EU funds and programmes, overall, the funding of CSOs and the media is fragmented, project-based and often comes from non-EU countries; whereas application procedures for financing should be transparent and accessible; whereas the Court of Auditors has concluded that the lack of a coherent EU media literacy strategy that includes tackling disinformation and the fragmentation of EU actions dilutes the impact of media literacy projects, and that many such projects have not demonstrated sufficient scale and reach;

Q. whereas fact-based journalism plays a key role in a democratic society, upholding the principles of truthfulness, accuracy, impartiality, honesty and independence; whereas freedom of expression and of information are fundamental rights guaranteed by the European Convention on Human Rights and recognised by the Charter of Fundamental Rights of the EU, as well as the International Covenant on Civil and Political Rights; whereas the tabloidisation of the media has a detrimental effect on the reliability of publically accessible information and the media landscape;

R. whereas whistleblowers, journalists, CSOs, activists and human rights defenders are

increasingly facing intimidation, intrusive surveillance and hacking, harassment and threats, including legal threats and abusive litigation; whereas they should be supported by the EU and its institutions; whereas strategic lawsuits against public participation (SLAPPs), including those initiated by authorities of third countries against EU nationals or EU-based entities, are a serious threat to democracy and fundamental rights such as freedom of expression and information, as they are a means by which to prevent journalists and activists as well as broader civil society actors from speaking up on issues of public interest and to penalise them for doing so, and thus have a chilling effect on all actual or potential critical voices;

S. whereas in the EU, there are cases of journalists whose existence and life are threatened as a result of their research into topics of public interest; whereas foreign powers are suspected of interfering in the Union and have extended repressive measures to territories within the Union in order to silence journalists who wish to report and denounce criminal acts; whereas an example of this is the strategy of judicial harassment being exercised by the Kingdom of Morocco against the Spanish journalist Ignacio Cembrero; whereas some journalists and human rights defenders that have been granted asylum in the EU are still the target of persecution, harassment, violence and assassination attempts; whereas the Member States should ensure their security and that they are able to continue their work;

T. whereas reducing the effectiveness of malicious information manipulation, and in particular its effects on the functioning of democratic processes, is a matter of public interest; whereas disinformation decreases the ability of citizens to take informed decisions and to freely participate in democratic processes; whereas this situation is intensified by the rapid development of new types of media; whereas according to the Media Pluralism Monitor 2022, no country is at low risk for the indicator of 'media viability', reflecting the existing economic threats to media pluralism; whereas news media operating in smaller markets, including local, regional and niche media, face additional challenges as they have limited revenues, and are becoming less viable using current commercial business models and cannot embrace new ones in the same way that media operating in larger markets can; whereas, in addition, some Member States, which Russia considers its sphere of influence, are more exposed to geopolitical risks arising from Kremlin interference in their information space;

U. whereas the promotion of media independence and pluralism and media literacy in tackling disinformation is one of the citizens' proposals contained in the final report of the Conference on the Future of Europe, published on 9 May 2022, where citizens called specifically for the EU to address threats to media independence through the establishment of EU-wide minimum standards as well as to defend and support free, pluralistic and independent media, to step up the fight against disinformation and foreign interference, and to ensure the protection of journalists; whereas the final report of the Conference of the Future of Europe also contained calls for setting up an EU body in charge of addressing and tackling targeted disinformation and interference, enhancing the cooperation of national cybersecurity authorities and legislation and guidelines for online platforms and social media companies to address disinformation vulnerabilities;

V. whereas the integrity of the internal market for media services may be compromised and the polarisation of society fomented by media providers that systematically engage in disinformation, including information manipulation and interference of state-controlled

media service providers financed by certain non-EU countries, such as China, Russia and Türkiye; whereas a highly concentrated and government-controlled media environment can lead to an informational autocracy, where the state or malign foreign actors can easily exert influence through the manipulation of information;

W. whereas China has invested almost EUR 3 billion in European media firms over the last 10 years, without an adequate response from the EU and its Member States; whereas China's example could be followed by other states with similar authoritarian political ideologies, entailing considerable risks for the integrity of European democracies and interference by other countries in the EU's domestic affairs; whereas a number of Chinese state-run Confucius Institutes, which spread propaganda and interfere in academic institutions, are still functioning in the EU; whereas Chinese broadcast media represent and disseminate the Chinese Communist Party's (CCP) ideology; whereas Chinese bot accounts are increasingly active on social media and in social networking, serving the needs of the Chinese authorities;

X. whereas a massive operation targeting international institutions, notably in Brussels and Geneva and serving Indian interests was recently uncovered by EU DisinfoLab, involving hundreds of fake media outlets and dozens of government-organised non-governmental organisations;

Y. whereas only some EU Member States have screening mechanisms for foreign media investments in place; whereas it is in the public interest to know about the beneficial ownership structures of media outlets;

Z. whereas important structural shortcomings facilitating information manipulation through online platforms still remain; whereas online platforms' business models are based on personal data, algorithms that push extreme and divisive content and advertising, whereby more engagement means more advertising revenue, and the drive for engagement rewards divisive and extreme opinions at the expense of fact-based information; whereas online platforms are therefore designed in a way that helps to amplify conspiracy theories and disinformation; whereas these global online platforms in addition have had a vast disruptive impact on the economic viability of the European media sector, as they dominate the advertising market, thus impacting media business models;

AA. whereas even though the Code of Practice on Disinformation was strengthened, many structural problems persist, such as the lack of binding rules and the provision whereby companies can choose their own commitments, which ultimately hinders the success of the Code of Practice as a tool;

AB. whereas rapidly evolving generative artificial intelligence (AI) technologies could have potentially grave consequences that could enable malicious actors to produce and spread more disinformation content, cheaper and at a greater speed; whereas particularly devastating effects could be faced by countries across the world that lack resources to address this challenge;

AC. whereas the Commission proposal on transparency and targeting of political advertising aims to address these structural problems in the context of political advertising;

AD. whereas platforms have developed several initiatives to counter online disinformation,

designing 'pre-bunking' campaigns to inform users about the dangers of disinformation by pre-emptively warning about and disproving false claims made through dis- and misinformation campaigns undertaken by malicious actors; whereas the effect of these initiatives cannot be fully evaluated owing to the absence of independent or institutionalised analyses by researchers with full access to the data;

AE. whereas non-English language content is still substantially left unmonitored as platforms still do not employ a sufficient number of reviewers and fact-checkers able to perform their respective tasks in other languages, especially in smaller languages in countries gravely affected by disinformation; whereas online platforms should guarantee fundamental rights to citizens, such as freedom of expression and of information;

AF. whereas since the takeover of Twitter by Elon Musk, the company has introduced a crisis misinformation policy, according to which the company would take action in response to tweets that contain false or misleading allegations regarding use of force and weapons, and that it would respond by prioritising tweets from state-affiliated media accounts and place a warning notice that a tweet has violated the company's crisis misinformation policy, but this approach was partially cancelled on 23 November 2022; whereas the company has fired the staff of all departments responsible for detecting, classifying or responding to disinformation, including a majority of content moderators and country-specific teams, and reinstated over 60 000 accounts which had previously been found to have broken the platform's rules by sharing disinformation, engaging in harassment or abuse, or running scams; whereas since the takeover, there has been an increase of abusive content of about 40 %; whereas there have been repeated and intolerable suspensions of the accounts of journalists and media outlets without concrete justification;

AG. whereas media reports on internal documents have raised questions about the political neutrality of the company's efforts to implement its policies against foreign interference and disinformation in the 2020 US presidential election, and whether those efforts also amount to a form of interference in the political and wider social debate around the election, as the dozens of internal emails revealed that methods intended to counter disinformation and hate speech were being used by the main parties in the United States to control the electorate; whereas it remains unclear how Twitter is going to develop in the near future, owing to concerning statements and decisions taken by its new senior management;

AH. whereas health dis- and misinformation is a serious threat to public health since it erodes public trust in science, public institutions, authorities and medical staff, as well as generating hostility towards them, and advances conspiracy theories; whereas such disinformation can be life-threatening when it deters people from seeking medically recommended treatments, including vaccinations, or promoting false treatments; whereas, during the COVID-19 pandemic, the amount of COVID-19-related content that was not dealt with after having been fact-checked and found to consist of mis- or disinformation amounted to 20 % in German and Spanish, 47 % in French, and 84 % in Italian; whereas smaller languages were even more heavily impacted;

AI. whereas networks of bots and fake accounts on social media platforms are used by malicious actors to undermine democratic processes; whereas Meta removed two networks originating in China and in Russia for violating its policy against coordinated

inauthentic behaviour; whereas the network originating in Russia and composed of over 60 websites impersonated legitimate websites of news organisations in Europe and posted original articles that criticised Ukraine, supported Russia and argued that Western sanctions on Russia would backfire; whereas similar findings were made by EU DisinfoLab in its Doppelgänger investigation; whereas this is only the tip of the iceberg and online platforms constantly have to be vigilant and to improve their content moderation policies;

AJ. whereas there is a lack of oversight over platforms such as Reddit and Telegram, where disinformation spreads mostly unchecked; whereas Spotify hosts podcasts containing mis- and disinformation content, in particular regarding vaccine disinformation; whereas some of them have up to 11 million listeners per episode; whereas the company has refused to take any actions against the accounts that broadcast the podcasts as it has no disinformation policy; whereas the EU has started multiple investigations into TikTok, concerning the transfer of EU' citizens data to China and targeted advertising aimed at minors;

AK. whereas the Digital Services Act (DSA) [1] entered into force on 16 November 2022 and will apply from 17 February 2024; whereas it fully harmonises the rules applicable to intermediary services in the internal market and contains specific provisions applicable to very large online platforms (VLOPs) and very large online search engines (VLOSEs) when it comes to systemic risks such as disinformation and manipulation;

AL. whereas the DSA creates obligations for VLOPs and VLOSEs to perform annual risk assessments and take measures to mitigate the risks stemming from the design and use of their services; whereas some provisions of the DSA should be extended to smaller platforms, on which disinformation keeps spreading unhindered;

AM. whereas the DSA classifies disinformation and election manipulation as systemic risks;

AN. whereas algorithms designed to benefit platforms' business models play a crucial role in the amplification of false and misleading narratives, creating filter bubbles that limit or distort the information available to individual users; whereas platforms still have not done enough to counter this; whereas the development, testing and functioning of algorithms still lack transparency;

AO. whereas social media platforms are used as tools, for example, to spread Russian propaganda seeking to justify Vladimir Putin's invasion of Ukraine, and to foster anti-democratic political movements in the Balkans; whereas AI, through the malicious use of large language models (LLM), such as ChatGPT, is becoming an increasingly important tool used to spread propaganda and disinformation, but will also be crucial to more effectively discover and counter manipulated narratives; whereas there is a need to develop digital technologies with respect for human rights and the rule of law;

AP. whereas the Commission set up a European Centre for Algorithmic Transparency, which is part of the Commission's Joint Research Centre, and is composed mainly of

[1] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1).

engineers and data scientists dedicated to the study of algorithms;

AQ. whereas digital services coordinators, which are independent authorities appointed by each Member State, have an important role and function and are responsible for supervising and enforcing the DSA in the Member States;

AR. whereas there is a risk of economic dependence, but also espionage and sabotage, with foreign companies acquiring influence over EU critical infrastructure; whereas Chinese shipping companies have acquired majority or sizeable interests in over 20 European ports, for example China Merchants Group in France and COSCO in the ports of Piraeus, Antwerp, Bilbao, Genoa, Hamburg, Rotterdam, Valencia and Zeebrugge; whereas the INGE 1 report called for a stronger regulatory and enforcement framework to ensure foreign direct investment (FDI) with a detrimental effect on the EU's security is blocked;

AS. whereas foreign actors, predominantly China and Russia, but also Iran, are actively trying to infiltrate European critical infrastructure and supply chains to steal information and/or know-how through espionage, in order to gain a competitive advantage or to sabotage parts of these infrastructures to impair their functioning; whereas the same malign behaviour is coupled with economic and infrastructure projects in candidate and potential EU candidate countries; whereas an increasing threat to European citizens also lies in the possibility of espionage and information gathering via everyday household appliances;

AT. whereas the EU's energy dependence on Russia has created enormous difficulties for its energy security after Russia started its war of aggression against Ukraine; whereas 'corrosive capital' projects by foreign actors in Member States, such as the Paks nuclear power plant in Hungary, risk influencing political decisions; whereas despite Russia's illegal occupation and annexation of parts of Ukraine in 2014, many EU countries increased their gas dependency on Russia; whereas some of these countries have recently reduced their dependency to almost 0 %;

AU. whereas the investment programmes for 5G deployment such as CEF2 Digital, as well as the 6G Programme of the Smart Networks and Services Joint Undertaking, could support technological sovereignty and reduce dependencies on foreign suppliers in this field by building secure 5G infrastructure as well as 6G technology capacities; whereas the development of critical technological infrastructure for the European economy should be reserved for European manufacturers and developers or those from like-minded countries;

AV. whereas national authorities of some Member States have strengthened their approach to countering foreign threats to critical infrastructure, such as espionage and sabotage;

AW. whereas disinformation and other information manipulation vitiates the public debate around elections and other democratic processes and can prevent citizens from making informed choices or discourage them from political participation altogether; whereas disinformation in political campaigns is a direct threat to fair democratic political competition; whereas these issues present a challenge to the 2024 European elections;

AX. whereas on the eve of the 2024 European elections increased interference and information manipulation activity is expected; whereas the European elections are

fundamental to the functioning of the democratic processes of the European Union, promoting its stability and legitimacy; whereas the democratic integrity of the Union must therefore be defended, including by preventing the spread of disinformation and undue foreign influence over European elections; whereas the proposal on the transparency and targeting of political advertising could make a contribution by establishing a ban on sponsors of political advertising coming from non-EU countries;

AY. whereas free and fair elections are a cornerstone of democratic countries, and independent and transparent electoral processes are necessary to foster a competitive electoral environment and citizens' trust in election integrity; whereas the systemic integrity of electoral processes is also entrenched in the legal and institutional frameworks governing how elections are conducted, including electoral management bodies; whereas the quality and the strength of these frameworks and democratic institutions are essential to the electoral integrity of any country; whereas online social platforms are increasingly important instruments in electoral decision-making;

AZ. whereas interference in electoral processes can occur in different ways, either direct or indirect, such as fraudulent operations with ballots, the blocking of entrances to polling stations or physical coercion to vote, the distribution of distorted information on candidates, the manipulation of or changes to election dates, and disinformation campaigns on social media, among others;

BA. whereas authoritarian regimes have become more effective at co-opting or circumventing norms and institutions that support basic liberties, and at providing aid to others who wish to do the same; whereas these regimes have fuelled and exploited polarisation, through proxies in third countries and in the EU, and have attempted to distort national politics to promote hatred, violence and unbridled power; whereas foreign interference in electoral processes is often not aimed exclusively at influencing specific election results but at undermining or destroying citizens' long-term confidence in the legitimacy of their democratic institutions as well as their democratic processes;

BB. whereas the Authority for European Political Parties and European Political Foundations contributes to the protection of the integrity of the European elections;

BC. whereas the European cooperation network on elections plays a crucial role in ensuring the integrity of the elections within the European Union; whereas this network has been set up by the Commission's services with the relevant Member States' services;

BD. whereas extra-EU funding of political activities and politicians inside the European Union before and after 24 February 2022, in particular from Russia, continues to be revealed by journalists and experts, puts at risk the integrity of the democratic functioning of the EU Member States and requires thorough investigation to hold those complicit accountable; whereas *El País* has revealed the involvement of the Iranian National Council of Resistance in the funding of far-right political movements in the EU; whereas Russia and Iran, together with other countries such as Venezuela, share a common goal of weakening democratic states;

BE. whereas the legislators are currently negotiating the proposal on political advertising which aims to complement the DSA, tackle the harmful fragmentation that currently exists in this area and help to strengthen our democracies in Europe and our democratic processes, allow citizens to make an educated decision during an election or referendum

through an open process and shelter EU citizens from disinformation, fake news, opaque political advertising techniques and foreign interference in general; whereas the legislators should reach an agreement on the proposal as soon as possible in order to ensure that the new rules are in place before the European elections in 2024;

BF. whereas in the first half of 2021 alone, there were as many recorded cyberattacks on EU institutions as in the whole of 2020[1]; whereas instances of attacks on EU and national institutions have increased following Russia's aggression in Ukraine, as exemplified by a cyberattack that hit the European Parliament during the November 2022 plenary session, shutting down the website after a vote on a resolution to declare Russia a state sponsor of terrorism;

BG. whereas the EU has significantly increased its efforts and investments in developing cybersecurity capacities, including through the EU programmes Horizon Europe and Digital Europe; whereas there is still a need for more efficient cybersecurity supported by the relevant funding; whereas strong cybersecurity infrastructure could reduce the costs of cyber-incidents; whereas the impact assessment of the proposed cyber resilience act estimates that the initiative could lead to a cost reduction from incidents affecting businesses of roughly EUR 180 to 290 billion[2]; whereas the Commission has been slow to take measures in response to the hacking of EU citizens in the EU with spyware by third countries, including of prominent figures such as heads of state or commissioners; whereas there is currently no action plan in place to prevent the hacking of EU citizens within the EU by people operating outside the EU;

BH. whereas the Council has recently adopted the NIS2 Directive to ensure a high common level of cybersecurity across the Union; whereas the NIS2 Directive has established the EU Cyber Crises Liaison Organisation Network (EU CyCLONe), which will strengthen the resilience of information systems; whereas a proper level of cybersecurity can only be achieved through the cooperation of multiple actors from the public and private sectors; whereas the EU still faces major dependencies in the field of cybersecurity;

BI. whereas the cyber defence of Ukraine requires the action and the cooperation of all partners; whereas western IT corporations have provided assistance to Ukraine in identifying vulnerabilities in its infrastructure; whereas there is a lack of technical capacities within the EU to identify vulnerabilities in its critical infrastructure; whereas cooperation and exchange of information with targeted partners, such as the US, the UK, Ukraine and Taiwan, is key to improving the EU's capacity to attribute attacks;

BJ. whereas the Smart Networks and Services Joint Undertaking was established in 2021 to enable European actors to shape global 6G standards; whereas collaboration between the Commission and Member State authorities on the implementation of the 5G cyber toolbox is ongoing in the framework of the Network and Information Systems (NIS)

---

[1] Impact analysis report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union (SWD(2022)0066). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0066.

[2] Executive summary of the impact assessment report accompanying the proposal of a pegulation for the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (SWD(2022)0282).

cooperation group; whereas the European Court of Auditors has concluded that since the 5G toolbox was adopted, progress has been made in reinforcing the security of 5G networks with a majority of Member States applying or in the process of applying restrictions on high-risk vendors, but that none of the measures put forward are legally binding, meaning that the Commission has no power to enforce them;

BK. whereas there have been instances of third countries transporting migrants and asylum-seekers to the EU's external border as part of their hybrid foreign interference strategies to challenge the EU and its Member States, such as in the autumn of 2021 by Belarus against Poland, Lithuania and Latvia; whereas these hybrid interference attempts also take the form of spreading disinformation by polarising the EU's societies and undermining European values and fundamental rights;

BL. whereas migrants, minorities and diasporas are frequently used by foreign actors, who orchestrate disinformation campaigns to exploit and amplify negative preconceptions about migration to build up tensions within European societies, such as with the Ukrainian diaspora being the victim of targeted Russian disinformation campaigns; whereas platforms play a key role in the dissemination of such information;

BM. whereas Europe is seeing a growing number of anti-gender movements, specifically targeting sexual and reproductive health, women's rights and LGBTIQ+ people; whereas such movements proliferate disinformation in order to reverse progress in women's rights and gender equality; whereas these movements have been reported to receive millions of euros in foreign funding, either public or private, including from Russia and the US;

BN. whereas this instrumentalisation of migrants and minorities at the EU's external borders highlights the importance of having an effective and integrated border management system and of applying operational, financial and diplomatic measures to remain resilient;

BO. whereas Parliament supports the Commission's proposal to include provisions on the instrumentalisation of migrants in the Schengen Borders Code, which will enable Member States to act in a more effective and coordinated manner;

BP. whereas Russian disinformation and propaganda campaigns also influence indirect opinion forming in Europe by focusing on the Russian-speaking diaspora in Europe and neighbouring countries; whereas Member States should play a key role in making fact-based news sources available for Russian-speaking population groups, in order to counter the pro-Kremlin narrative; whereas Russian disinformation and propaganda campaigns are also widespread in numerous post-Soviet countries, including in Central Asia;

BQ. whereas the Belgian federal prosecutor's office has opened an investigation regarding suspicions of money laundering, corruption and participation in a criminal organisation originating from third countries; whereas several arrests and searches took place from 9 December 2022 onwards, affecting both current and former Members of the European Parliament, as well as staff; whereas these allegations need to be followed by effective measures by Parliament and the other EU institutions to close the loopholes for foreign interference, as well as to increase transparency and accountability in order to protect the integrity of the institutions;

BR. whereas trust in Parliament's integrity and the rule of law is paramount for the functioning of European democracy; whereas it is key to ensure that democratic processes are not captured by private and external interests and that citizens' rights are fully respected; whereas the ability of interest and group representatives to influence decision-making in Parliament by way of arguments is a vital part of European democracy;

BS. whereas the INGE I report already highlighted that there is a serious lack of legally binding rules regarding lobbying and enforcement of the EU's lobbying register, and that former high-level European politicians and civil servants are often hired or co-opted by foreign authoritarian state-controlled national or private companies; whereas this makes it practically impossible to track lobbying coming from outside the EU;

BT. whereas the capture of elites by foreign interests, facilitated by the non-restriction of "revolving doors" between the EU institutions and autocratic countries with a high risk of harmful interference against the democratic interests of the Union, continues to represent a significant form of foreign interference in the democratic functioning of the European Union and can be considered an issue related to corruption;

BU. whereas China and Russia have imposed sanctions on European researchers and research institutions owing to their writings or views;

BV. whereas more clarity is needed regarding foreign influence through interest representatives at the EU level, especially in cooperation with non-governmental organisations (NGOs), consultancies, foundations, think tanks and private companies; whereas this should not prevent the normal outreach activities of embassies; whereas the number of Russian Embassy staff is decreasing around Europe, while it keeps rising in Budapest, proving that Hungary is susceptible to Russian intelligence activities;

BW. whereas lobbying on behalf of foreign interests, especially when it concerns companies in strategic sectors and their governments, may open the door to foreign interference in our institutions; whereas the Transparency Register was significantly strengthened following an interinstitutional agreement; whereas strengthening transparency requirements for CSOs, consultancies, foundations, think tanks and private companies could serve the purpose of detecting foreign interference;

BX. whereas there have been several cases of hostile intimidation and harassment campaigns against Members of the European Parliament orchestrated and coordinated by foreign countries; whereas countries such as Russia, China and Iran have put entry bans and sanctions on individual Members and bodies of the European Parliament and Member State parliaments, because of their criticism to the respective governments' human rights policies;

BY. whereas some authoritarian states are falsely accusing European citizens of having committed crimes or offences and are holding them in prison in order to influence the decisions of EU Member States; whereas citizens are currently being held and convicted in Iran without any justification, including the Swedish national Ahmadreza Djalali and seven French nationals;

BZ. whereas in March 2022 the EU imposed sanctions on the Russian propaganda outlets Russia Today (RT) and Sputnik, temporarily suspending their broadcasting activity, as

well as ordering internet access providers and search engines to block access and search engines to de-index their content; whereas since the adoption of the ninth package of sanctions, satellite operators such as France's Eutelsat and Luxembourg's SES have ceased to provide broadcasting services in the EU to RT and Sputnik; whereas Eutelsat 36B continues to broadcast programming by Russian Trikolor and NTV plus in the Ukrainian territories occupied by Russia; whereas SES continues to broadcast RT News in India, Mexico and South Africa; whereas other national satellite operators such as Hellas Sat and Hispasat, as well as Hungarian national channels, continue to broadcast sanctioned TV channels; whereas RT France and RT News are still available online; whereas Russian propaganda is often amplified by various international media outlets with very wide reach in certain regions of the world;

CA. whereas in clear contradiction of the EU's imposed sanctions, Serbia, an EU candidate country, has become a safe haven for some Russian companies looking to evade or weather out sanctions imposed by the EU, as since July 2022, Belgrade has been hosting multiple offices of RT (formerly Russia Today), which has launched its online news service in Serbian;

CB. whereas criminalisation of foreign interference would target and stigmatise this malign behaviour; whereas there is currently no general prohibition on foreign interference in the EU, meaning that perpetrators may engage in it without fear of penalty, unless their conduct amounts to an existing offence; whereas pursuant to the third subparagraph of Article 83(1) of the Treaty on the Functioning of the European Union (TFEU), on the basis of developments in crime, the Council may adopt a decision identifying other areas of particularly serious crime with a cross-border dimension; whereas there is a need to impose sanctions and place restrictions on perpetrators of foreign interference to prevent them from taking future actions;

CC. whereas the Commission has proposed to harmonise criminal offences and penalties for the violation of EU sanctions; whereas a number of Member States have considered extending the competences of the European Public Prosecutor's Office in order to cover these violations;

CD. whereas the EU has already developed several important pieces of legislation to counter malign foreign information manipulation and interference (FIMI); whereas there is a danger that EU regulatory frameworks to combat disinformation may be copied and might be selectively used by other (authoritarian) countries in order to curb media freedom and freedom of expression; whereas an evaluation of the effectiveness and impact of existing instruments on the strengthening of societal resilience has not been properly undertaken at EU level; whereas such an evaluation would further improve the orientation of future policies and tools to address foreign interference and hybrid threats;

CE. whereas, following its economic growth and political expansion on the global stage, China is trying to maximise the diffusion of its propaganda abroad, spreading positive narratives regarding the country while simultaneously attempting to suppress critical voices; whereas China is taking control of all of the traditional media information channels in Africa, which are still the continent's most used tools for accessing information; whereas Russia is also expanding its disinformation operations in Africa; whereas the Wagner Group is directly involved in those operations; whereas those operations could jeopardise the safety of European citizens and the development of

cooperation with African partner states;

CF. whereas the EU is taking a leading role in the work of the UN Ad Hoc Committee on Cybercrime, under the UN Third Committee, with the aim of safeguarding the fundamental and procedural rights of suspects;

CG. whereas the overall awareness of the dangers of information manipulation and interference in other countries in the world has grown since the COVID-19 pandemic; whereas the UN has proposed several initiatives to enhance governance in the digital sphere and create more coherence among UN member states, such as the Global Code of Conduct to promote the integrity of public information and the Global Digital Compact;

CH. whereas in discussions with the ING2 Special Committee, representative of some platforms and other stakeholders have reacted positively to the establishment of global standards, and in particular European and, when possible, transatlantic standards, in countering FIMI;

CI. whereas successful common foreign and security policy (CFSP) / common security and defence policy (CSDP) missions and operations and EU delegations abroad are among the best strategic communication campaigns by the EU in non-EU countries;

CJ. whereas the Council approved the Strategic Compass in March 2022; whereas the Strategic Compass outlines that by 2024 all CSDP/CFSP missions and operations should be equipped with sufficient strategic communications tools and resources to counter FIMI; whereas a process of modernisation and professionalisation in missions communication is required, including supporting initiatives to combat disinformation vulnerabilities; whereas the European External Action Service (EEAS) Strategic Communication Task Force (StratCom) has stepped up its cooperation with CSDP missions and operations to help them detect, analyse and understand FIMI campaigns;

Coordinated EU strategy against foreign interference

1. Underlines that Russia's war of aggression against Ukraine brought to the fore the links between attempts at foreign manipulation of information and threats to the EU and its immediate neighbourhood, Western Balkans and Eastern Partnership countries, as well as to global security and stability; notes that Russia's full-scale war in Ukraine made the effects of Russia' interference in democratic processes, which began long before the invasion and is based on historical revisionism, even more obvious;

2. Stresses the need to develop the EU's open strategic autonomy in order to limit opportunities for interference through EU dependence in strategic sectors such as energy, digital technology and health; supports the efforts of the European Commission, the Council and other institutions in this respect, particularly in the context of REPowerEU and the EU Digital Agenda;

3. Takes notes of the Commission's follow-up of the first recommendations adopted by Parliament on 9 March 2022; reiterates, however, its call for a coordinated EU strategy to tackle foreign interference, taking into account both the complexity and the multi-dimensional nature of the threats, based on an articulated and multipolar geopolitical analysis; considers that this whole-of-society strategy should include measures to

enforce existing provisions on foreign interference better, create a focal point for investigation and strategic responses to counter foreign interference, and secure funding for capacity-building activities to tackle disinformation and uphold democratic processes; believes this strategy should bring together and create synergies between isolated efforts, strategies, action plans, roadmaps and underlying projects and funding streams; believes it should establish the strategic goals, necessary mandates and operational capabilities, such as threat information sharing and technical attribution, the legislative and diplomatic tools, such as new legislation, norms, toolboxes, political attribution, sanctions, and other countermeasures, as well as capacity-building requirements, such as additional funding of EU agencies and CSOs that contribute to these efforts with key performance indicators to ensure that sufficient scale and reach of results is obtained;

4. Welcomes in this regard the announcement by the President of the Commission of a Defence of Democracy package; recalls the Commission's statements to carefully take into account INGE and ING2 committee recommendations that a robust Defence of Democracy Package be developed together with legislation to counter hybrid threats in the EU;

5. Calls on the Commission and the member States to ensure that all measures taken to protect the EU against foreign interference and information manipulation need to include strong and resolute safeguards to fundamental rights, including the freedom of expression and the freedom of opinion;

6. Is of the opinion that efforts to move from a country-agnostic approach that treats all foreign influence efforts in the same way, regardless of their source country, towards a risk-based approach based on objective criteria should be given careful consideration, similarly to the Directive (EU) 2015/849[1] , and lessons drawn from other countries; believes the risk-based approach would function as one of the building blocks of a tiered approach that informs policies and countermeasures against foreign interference, removes unnecessary legal complexity, and uses the limited capabilities and resources, from operational to policy level, more efficiently by taking into account the very factor that matters most in evaluating and responding to foreign influence, namely its source country; believes also that this approach should include a clear set of potential sanctions, and therefore function as a form of deterrence towards transgressors and as leverage towards emerging malicious actors that could be added to the list; considers that potential criteria could include:

   (a) engagement in activities of foreign interference,

   (b) an intellectual property theft programme directed against the EU and its Member States,

   (c) legislation that forces national non-state actors to participate in intelligence

[1] Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015, p. 73).

activities,

(d) consistent violation of human rights,

(e) revisionist policy towards the existing international legal order,

(f) enforcement of authoritarian ideology extraterritorially; calls on the Commission and the EEAS to present specific recommendations for introduction of this approach and direct them to the Council for approval;

7. Considers that the EU, in collaboration with the Member States, should step up its strategic communication on countering and debunking, information manipulation by widely reporting ongoing operations as they happen (debunking), in particular in the Global South; calls for strengthening of and further investment in EU prebunking capabilities; recalls the examples set by Ukraine and Taiwan in pre- and debunking information manipulations and the need to build on the lessons learned from their experience; recalls similarly that in order to prebunk or rapidly debunk information manipulation, there needs to be a framework for rapid sharing of information provided by civil society and private companies;

8. Supports Vice PresidentVěra Jourová's public call in Tallinn in January 2023[1] for independent communication channels for Russian speakers to be expanded; calls on the Commission and the EEAS to follow up with concrete proposals and measures accordingly;

9. Condemns the dangerous phenomenon of disinformation-for-hire, whereby providers offer disinformation services to government and non-government actors, for example over the dark web, setting out lists of services and prices; deplores that this kind of service has been used to attempt to undermine electoral processes, among many other uses;

10. Calls for the establishment of an EU structure tasked with analysing statistical data, coordinating research projects and producing reports to increase situational awareness and threat intelligence sharing, attribution and countermeasures in relation to FIMI, including involving the EU's external action service, and which serves as a reference point and specialised knowledge hub to facilitate and foster operational exchange between Member States' authorities, EU institutions, and EU agencies; considers that this structure should be financed from the EU budget and take the form of a Centre for Information Integrity that collaborates with all EU institutions in using all available tools to avoid duplication;

11. Calls on the Member States to acknowledge the fact that foreign interference, including disinformation, is a national and cross-border security threat; stresses the need for solidarity between the Member States so that such activities can be effectively combated; calls for Article 222 TFEU to be amended to include foreign interference;

12. Calls for the national parliaments of the EU Member States to consider establishing their own parliamentary bodies tasked with overseeing actions related to the protection of their democracy against foreign interference and information manipulation, and to set

[1] Vice-President Jourová speech on Defending EU values in the time of the war.

up regular exchanges on these topics;

13. Notes with interest the conclusion of the EU Integrated Resolve 2022 joint exercise, which aimed to boost the EU's ability to respond to a complex, hybrid crisis with both an internal and an external dimension; regrets, however, that Parliament was not involved in this exercise and calls on the other EU Institutions to involve Parliament in the structure of all exercises of this kind;

14. Encourages all types of cooperation between the services of the different EU Institutions in charge of operational activities concerning monitoring and counteracting disinformation, such as that existing between Parliament's task force on Disinformation, Commission services and the EEAS StratCom division with its Rapid Alert System; welcomes the engagement of the EEAS and the Commission with Parliament to regularly update it on significant developments in the FIMI threat landscape, especially when it concerns EU elections; suggests the establishment of a Rapid Alert System for Members of the European Parliament and members of national parliaments to counter disinformation on online platforms and prevent the sharing of disinformation;

15. Welcomes the facilitation by the EEAS of an Information Sharing and Analysis Centre (ISAC) to develop a common methodology and framework for the collection and sharing systematic threat intelligence and evidence and ultimately provide better situational awareness; highlights the progress made by the EEAS on a common analytical framework and methodology on FIMI as described in the EDAP and underlines how, as part of the ISAC, such an open-source, collaborative and interoperable protocol to support situational awareness can contribute to closer collaboration among EU institutions, bodies and agencies (EUIBAs), Member States, social media platforms, news agencies, and civil society actors; calls for sufficient funding to be channelled towards the continuous development, involvement of society, and capacity-building that contributes to the wide adoption of this model with significant reach and scale across the Union;

16. Calls for a permanent body in the European Parliament to ensure a transversal approach to effectively monitor and fight foreign interference;

Resilience

17. Calls for a collective effort by the EU institutions, Member States, partner countries, civil society, the business world and independent media to raise social and institutional awareness and invest in education about disinformation, information manipulation and foreign interference and how to counteract it, in a holistic way;

18. Underlines that the EU must learn lessons from Ukraine's, Taiwan's and other countries' experience and expertise in countering foreign interference and aggression and continue close cooperation with such countries in this field; notes however the different context in which Taiwan operates;

19. Welcomes the fact that the European Digital Media Observatory (EDMO), an independent network for fact-checkers, academic researchers and other stakeholders, will soon have hubs covering all EU Member States, thus reinforcing its mission in detecting and analysing disinformation campaigns, misinformation and other content created by third countries with clear propagandistic intent, and organising media

literacy activities and other activities supporting the fight against disinformation; emphasises the potential need for a legal framework in the EU or in the Member States to ensure quality fact-checking;

20. Reiterates its call for Member States to include media and digital literacy, civic education, common European history, respect for fundamental rights, critical thinking and the promotion of public participation on school and university curricula, in parallel with general efforts to raise awareness among adults, including the elderly, and efforts to bridge the digital divides based on age, gender and socio-economic status; calls for a concerted EU media literacy strategy with projects that create tangible results with significant scale that reach the whole Union; encourages the sharing of EU Guidelines for Media Literacy with candidate countries, translated into national languages, to tackle disinformation and promote digital literacy through education and training; asks Member States, in this regard, to consider developing and distributing, within educational institutions, educational materials aimed at different age categories from which children and young people alike can learn how to inform themselves properly and how they can check the accuracy of information; calls for the creation of an observatory of foreign influences and their impact on higher education and research;

21. Highlights the importance of historical remembrance and research on totalitarian regimes, such as on the Soviet regime, and a transparent, fact-based public debate about such regimes' crimes in order to strengthen the resilience of our societies against distortions and manipulations of history; reiterates the importance of CSOs, such as Memorial, working in the field of historical remembrance, particularly with regards to recent European history, which is the target of systematic disinformation and revisionism by Russia in its efforts to justify its ongoing interference and aggression;

22. Calls on the Commission to develop an effective Defence of Democracy Package, taking into account the unique Conference on the Future of Europe experience and final proposals, including the initiatives to strengthen our democracy from within, by nurturing a civic culture of democratic engagement and active participation by citizens at all times, including outside the election period;

23. Underlines the need for public administrations at all levels to have specific training on identifying and countering acts of information manipulation and interference, and emphasises that this training should be gender-sensitive; reiterates the call on EUIBAs and on national authorities to continue and strengthen similar training and current situational awareness actions as hybrid threats are persistent and widespread and increasingly aimed at influencing EU policies and legislation; calls on EUIBAs to set up interinstitutional training to promote the overall resilience of EUIBAs as a whole;

24. Calls on EUIBAs and national authorities to adopt a dedicated communications framework containing measures to rapidly detect foreign interference and attempts to manipulate the information sphere in order to prevent and counter such attempts; welcomes the role of the EEAS, NATO StratCom CoE and Hybrid CoE as important partners in developing increased situational awareness and additional responses to counter FIMI;

25. Reiterates its call on the EEAS to build its expertise on strategic communication and public diplomacy, which requires a strengthened mandate and the allocation of more resources to its Strategic Communication division and its task forces in particular,

following a risk-based approach and taking into account the Russia's ongoing war of aggression against Ukraine and the hybrid warfare and propaganda coming from both Russian state and non-state actors, as well as the impact of that hybrid warfare on EU candidate countries in the Western Balkans, and on Moldova and other Eastern Partnership countries; stresses that dialogue with citizens is indispensable in order to raise awareness about the EU's foreign and security policy priorities; acknowledges and praises the work on the EUvsDisinfo website and database, and calls for further expansion of this platform with appropriate funding;

26. Notes the urgent need to step up efforts to counter malign FIMI campaigns aiming to limit EU candidate and potential candidate countries' abilities to progressively align with the EU's common foreign and security policy (CFSP); welcomes the contribution of the EEAS in supporting institutional capacity and transparency of media ownership, specifically in the Western Balkans, taking into account the fragile security situation and the risk of spillovers; underlines the need to proactively counter malign actors' propaganda in the region, which aims to undermine EU interests and values;

27. Calls for the EU and Member States to step up support for CSO efforts on countering FIMI, as they have proven effective at raising awareness of the risks associated with information and disinformation transmitted via social media, in particular, and they have also shown themselves to be effective in the case of traditional media, as many CSOs operate at local level, so are closer to the targets of disinformation and know better how to communicate with them; believes that technology and media companies should engage with CSOs, who are able to provide expertise on political and cultural contexts, in order to devise strategies to mitigate risks of interference in electoral processes;

28. Calls for sufficient and sustainable funding to be made available, in a clear and transparent manner, to investigative journalists and CSOs commensurate with their efforts to raise awareness, expose efforts to interfere in democratic processes and neutralise their impact;

29. Calls for the earmarking, boosting and leveraging of public sources for the relevant CSOs, and also for efforts to increase private funding such as facilitating a conference of donors; calls for a joint initiative to be launched bringing together EU funds and programmes, including the upcoming Defence of Democracy package, along with financial organisations, bilateral donors and beneficiaries, so as to enhance harmonisation and cooperation in investments for democratic resilience and countering FIMI, and that this investment framework should provide tailor-made grants, on the basis of objective, transparent and monitored criteria for independent fact checkers, investigative journalists, academics, think tanks and CSOs engaged in increasing situational awareness (such as researching, investigating, and identifying the origin of information manipulation and interference, developing cooperation in the field as well as developing and operationalising ISAC methodologies and open-source tools to tackle the challenge of FIMI) and include measures to promote media, digital and information literacy, as well as other resilience-building activities and support for human rights defenders through annual or bi-annual calls for proposals that would cover long-term multi-year funding;

30. Emphasises that it is essential that whistleblowers, journalists and other media professionals are guaranteed the necessary conditions to contribute to an open, free,

impartial and fair public debate, which is vital for democracy and a key aspect of helping society counter disinformation, information manipulation and interference; emphasises the need for secure equipment and strong, open source, end-to-end encryption to protect the confidentiality and integrity of communications between journalists and their sources;

31. Welcomes the anti-SLAPP proposal[1], consisting of a proposal for a Directive and a recommendation to improve the protection of journalists, human rights defenders and CSOs from abusive court proceedings; welcomes furthermore the analysis made by the Commission in its 2022 Rule of Law Report of existing threats against the safety of journalists in the EU and legal threats and abusive court proceedings against public participation; highlights the rise in spyware surveillance of journalists and CSOs in the EU as a means of intimidating and harassing them; stresses the need to include this dimension in the Commission's assessment on rule of law;

32. Recalls that independent, pluralistic, quality media services are a powerful antidote to FIMI; recalls in that regard the Journalism Trust Initiative, established by Reporters without Borders, which aims to set industry standards; reiterates its call for a permanent EU news media and magazine programme; considers that media freedom and pluralism must also be protected and promoted in the online environment, in particular as regards the availability of journalistic content on online platforms;

33. Notes the need to ensure that the fight against disinformation also involves traditional newspapers and news channels; calls in particular for news channels to be more transparent about the profile of the experts they invite on their sets;

34. Welcomes the Commission's proposal for a European Media Freedom Act[2] (EMFA) with a view to establishing a common framework at EU level to guarantee pluralism and independence in the internal market for media services by laying down specific provisions against political interference in editorial decisions and against surveillance, as well as ensuring adequate funding of public service media outlets, the transparency of media ownership, and protecting media content online; urges that measures also be put in place to protect the media and its workers, especially when targeted by foreign powers seeking to undermine the right to information; underlines that the provisions on surveillance in particular still require substantial improvements to ensure that they do not legitimise the use of spyware against individuals, notably journalists, and thereby undermine fundamental rights instead of strengthening them;

35. Welcomes the proposed creation, within the framework of the EMFA proposal, of a new European Board for Media Services bringing together national media authorities, which should play a significant role in the fight against disinformation, including foreign interference and information manipulation; notes, in particular, that one of the board's proposed tasks is the coordination of national measures on the provision of media services by providers established outside of the EU that target audiences in the

---

[1] Proposal for a directive on protecting persons who engage in public participation from manifestly unfounded or abusive court proceedings ('Strategic lawsuits against public participation') (COM(2022)0177).

[2] Proposal for a regulation establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU (COM(2022)0457).

EU and that may present a risk to public security; recommends that the countries of the Western Balkans and the Eastern Partnership be included in the remit of the board in this regard; urges that the European Board for Media Services must be independent from the Commission and Member State governments, in terms of both its organisation and financing, so it is able to work objectively and politically independently;

36. Welcomes, in connection with the EMFA, the proposals for independent monitoring of the internal market for media services, which would include detailed data and qualitative analysis of the resilience of the Member States' media markets, in particular as regards the risks of FIMI; welcomes the proposal to organise a structured dialogue between platforms and the media sector to monitor platforms' compliance with self-regulatory initiatives; stresses the importance of ensuring that the EMFA or any other current or future media or tech legislation does not include special exemptions from horizontal content moderation rules giving a blank cheque to those who spread disinformation;

37. Calls for the establishment of 'mirror clauses' whereby the openness of the European information space to third countries would be proportionate to the access European media outlets have in these countries; encourages the Commission to develop an EU-wide regulatory system to prevent media companies that are under the editorial control of foreign governments or owned by high-risk foreign countries from acquiring European media companies; this should apply predominantly to non-democratic or high-risk countries in which European media organisations are not allowed to operate freely, or are pressured to tilt their coverage in favour of national governments; these efforts should be based on a common database to facilitate harmonised prevention and/or prosecution across the European Union; suggests that such a regulatory system can be based on existing FDI screening mechanisms to prevent duplications; encourages the inclusion in the EMFA of the provisions on media ownership transparency that are currently in the recommendations;

38. Underlines that the increase in climate change denialism can be linked to a wider embrace of conspiracy theories in the public discourse that is based on the deliberate creation of a counter reality and the rejection of science, and which includes false ideas about everything from Russia's war of aggression against Ukraine to COVID-19 vaccines; emphasises the role of foreign actors in disseminating disinformation about climate change and EU climate policy, which is undermining public support and is also being used in the narratives of domestic actors who exploit climate disinformation for their own political ends;

39. Supports the call made by leading climate experts at the 27th Conference of the Parties of the UN Framework Convention on Climate Change (COP 27) for tech companies to tackle the growing problem of disinformation, and in particular to accept a universal definition of climate mis- and disinformation that encompasses the misrepresentation of scientific evidence and the promotion of false solutions, to commit to the goal of not publishing any advertising that includes climate mis- and disinformation and greenwashing, and to share internal research on the spread of climate mis- and disinformation and greenwashing on their platforms;

40. Calls on platforms to take measures to enhance transparency and prevent and ban the placement of advertising promoting climate change denial and apply them to conspiracy theories and disinformation; recognises that there is an urgent need to demonetise the

spread of the disinformation economy around climate change;

41. Notes with concern that many of the most high-traction amplifiers of climate change denial and attacks on climate action have 'verified' status on various social media platforms, including Twitter, allowing them to spread mis- and disinformation under this privileged status to millions of followers and that such amplifiers are often based outside of the European Union; calls on Twitter to implement stricter checks when selling its 'blue check' marks;

Interference using online platforms

42. Recalls that the business model of online platforms still relies on advertising based on personal data and opaque algorithms whereby more engagement translates into more advertising revenue, and that this engagement is generated by algorithms that reward polarised and extreme opinions at the expense of fact-based information and thus pose significant risks of data manipulation; stresses that the General Data Protection Regulation[1] (GDPR), the DSA, the Code of Practice on Disinformation and the upcoming Regulation on Transparency and targeting of political advertising create additional safeguards against such abusive and manipulative practices; recalls the support for all measures to ban micro-targeting for political advertising, particularly but not limited to those based on sensitive personal data;

43. Calls on the Commission, Member States and tech companies to work together and to invest more resources in developing regulatory and technological remedies to AI-powered disinformation;

44. Regrets that larger platforms, such as Meta, Google, YouTube, TikTok and Twitter, are still not doing enough to actively counter disinformation, and are even laying off staff despite constant calls from regulators, civil society and even internally from company staff responsible for integrity; recalls that platforms must have sufficient personnel to ensure regular updates to moderation tools in order to prevent harmful content circumventing their moderation policy; recalls that disinformation and interference campaigns rely strongly on cross-platform coordination of disinformation and micro-targeting; regrets the fact that the EU is dependent on non-EU companies to help preserve the integrity of European elections; as the self-regulatory approach of the CoP has fallen short, urges all platforms, including smaller ones, to step up their coordination to better identify campaigns and prevent their spread;

45. Regrets that social media companies are not honouring their responsibilities and are proving inefficient at identifying misinformation and disinformation on their platforms and are slow to take it down when they do; laments that this inactivity by online platforms is an expression of a lack of binding rules in the European regulatory framework; recalls that the platforms' business model implies that they have access to the relevant data; regrets that they often only act when citizens, researchers or the media flag specific content; calls on platforms to prioritise fact-based information coming

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

from reliable sources;

46. Calls on platforms to allocate more qualified staff, resources and capacity to monitor and moderate harmful content and behaviour in all EU official languages, local languages and dialects, and encourages platforms to increase funding and improve the integration of accredited third-party fact-checkers in all EU languages; underlines the urgent need to address harmful content;

47. Notes that it is also highly regrettable that big tech platforms do not offer human-to-human customer service in most EU Member States;

48. Denounces Twitter's backward steps in the fight against disinformation since its change of ownership; deplores, in particular, the fact that Twitter has significantly reduced the number of staff responsible for disrupting disinformation, including those responsible for global content moderation, hate speech and online harassment; deplores the recent reinstatement of suspended accounts without a proper assessment and particularly the reinstatement of violent right-wing and openly fascists accounts, including those that deny the outcome of the US presidential elections in 2020; strongly repudiates Twitter's decision to stop enforcing its policy against COVID-19 disinformation;

49. Notes that Russia's war of aggression in Ukraine has highlighted the lack of contact points for authorities to report disinformation and illegal content; deplores that Meta management has often transferred the responsibility for content moderation to the security team based in the United States; is concerned by the fact that there are only two representatives of Meta in the Baltic countries, meaning there are insufficient resources to moderate content, leading to errors such as the banning of legitimate accounts;

50. Finds it worrying that health disinformation groups, political extremists and religious fundamentalists such as the Taliban have been able to obtain 'verified' status with a check mark by subscribing to 'Twitter Blue'; calls on Twitter to amend its policy in order to prevent impersonation, falsification or misleading claims of expertise;

51. Recalls that Twitter is a signatory to the strengthened Code of Practice on Disinformation, and that a change of ownership should not have an impact on the platform's commitments under the Code; reminds Twitter that the company must abide by all relevant European Union regulations, including the DSA; urges the Commission and competent national authorities to ensure that Twitter abides by EU standards and rules and to apply appropriate sanctions if tech companies fail to comply with EU standards;

52. Calls on platforms to facilitate full access, in particular to researchers, to the data underpinning the findings and to keep a repository of take-downs to help researchers in future investigations, as well as to help other tech companies, democratic governments and law enforcement authorities take appropriate action; calls on the Commission to ensure this occurs in the framework of the DSA and the Code of Practice on Disinformation and to require platforms explain why they considered it not to be technically feasible to provide access to data;

53. Welcomes the DSA provisions that require VLOPs and VLOSEs to provide information on algorithms, requiring them to explain how they work so it is possible to assess their impact on elections and other democratic processes, and to take the necessary risk-

mitigation measures; calls on the signatories of the Code of Practice on Disinformation to fully honour their commitments; regrets the lack of binding commitments for the signatories to the Code of Practice on Disinformation; calls for the swift adoption of the CoP as a code of conduct under the DSA, including audits that would assess compliance as stipulated under Article 28, and for the Commission to consider what new legislative proposals or updates are required to fill the compliance gap, as well as to provide for the possibility for temporary or permanent suspension of platforms that systematically fail to comply with their commitments under the CoP;

54. Is concerned that some actors whose services contribute significantly to the dissemination of disinformation are not signatories to the CoP, such as Apple, Amazon, Odysee, Patreon, GoFundMe, and Telegram; calls on the Commission to encourage remaining relevant stakeholders to sign and fully comply with the CoP and take part in its task force; calls for a legal framework to be established in order to ensure a minimum level of commitments to fight disinformation on these services; is concerned by the fact that Telegram does not cooperate at all with policymakers in democratic countries and has been reluctant to work with CSOs;

55. Welcomes the fact that all the players in the online advertising ecosystem are committed to controlling and limiting the placing of advertising on accounts and websites disseminating disinformation or placing advertising adjacent to disinformation content, as well as to limiting the dissemination of advertising containing disinformation, and that this commitment also extends to political advertising; highlights, however, that there is still insufficient data to confirm whether the measures taken are bringing results; regrets that this business model and the recommender algorithms that underpin it remain crucial enablers of the spread of disinformation and false, misleading and incendiary content; is concerned by the willingness of platforms to use the pretext of 'empowering' users as a way of shifting responsibility for limiting the placement of advertising on accounts and websites disseminating disinformation onto them; whereas this responsibility should fall on the platforms, as they have the relevant data and expertise, as long as their actions remain transparent and the data is made available to researchers; is worried by the lack of transparency in the market for brand protection tools addressing image-related risks, as these tools often rely on algorithms that have been found to mislabel legitimate and trustworthy news outlets;

56. Is concerned about the use of footage created using video games to spread disinformation about the Russian invasion of Ukraine and other armed conflicts; calls on media outlets to be more vigilant about such content and to develop effective means of removing it from their platforms; is concerned that Russian-based video and online game companies, including those producing mobile games, are still operating freely on European markets and could be used to spread disinformation and propaganda;

57. Calls for the swift adoption of the CoP against disinformation as a Code of Conduct (CoC) under the co-regulatory mechanism of the DSA, bearing in mind that its success will depend on strict enforcement in the case of underperforming signatories through mandatory audits under Article 28 of the DSA; calls for harmonisation of the different user appeals mechanisms and the commitments on over-moderation as well as under-moderation;

58. Recalls that state authorities have accounts on social media platforms including accounts used for policing purposes and to monitor disinformation trends; notes that, as

long as these accounts do not engage in interactions with other users, they should be identified as safe and should not be taken down by platforms;

59. Calls for individuals and legal entities to be able to sue platforms for inaction when misinformation or disinformation are not taken down, in particular when they are targeted by it;

60. Supports the establishment of independent platform rating agencies to inform the public about platforms' practices so that people can make an informed choice when registering to use them;

Critical infrastructure and strategic sectors

61. Welcomes the recently agreed CER Directive, the Council's recommendation to strengthen critical infrastructure, and the NIS2 Directive; welcomes its expansion to cover critical infrastructure in the area of food production, processing and distribution; believes that recent attacks, such as the sabotage of critical infrastructure and increased cyberattacks show the need to evaluate existing legislation once implemented in Member States and calls on the Commission to come forward, if necessary, with additional strengthened proposals, which should include building the resilience of civil society organisations working to counter foreign interference and disinformation; additionally, calls on all Member States to rapidly update their national security strategies and undertake stress tests on their critical infrastructure to identify weak points; reiterates its recommendation to extend the list of critical entities to include digital election infrastructure and education systems;

62. Is concerned about the EU's dependence on foreign actors and foreign technologies in critical infrastructures and supply chains; points to vulnerabilities created by FDI being used as a geopolitical tool; reiterates its call on the Commission to develop ambitious binding ICT supply chain security legislation that includes non-technical risk factors, following up on the Council's proposal, and a stronger regulatory framework to the FDI Screening Regulation[1]; believes that the stronger regulatory framework with guidelines for further harmonisation of national FDI screening practices should include the prevention of takeover of critical companies in vital sectors or media companies by foreign parties that are under the direct or indirect control of high-risk countries and that the addition of outbound investment should be considered for inclusion under the scope of the instrument; calls on the Member States to establish ownership transparency registers; believes that the Commission, subject to supervision by the Council, should be able to block FDI that might be detrimental or contrary to EU projects and programmes or other EU interests; underlines that in the Western Balkans investments of this nature could push countries into debt traps, further destabilising the region;

63. Notes that despite such FDI screening mechanisms, Chinese companies such as Nuctech have been granted contracts in European critical infrastructure, leading to security risks; calls therefore on the Council and the Commission to exclude the use of equipment and software from manufacturers based in high-risk countries, particularly China and Russia, such as TikTok, ByteDance Huawei, ZTE, Kaspersky, NtechLab or Nuctech;

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

calls on vital sectors and other sensitive sectors to exclude the use of hardware and software from high-risk countries that can be used to threaten the confidentiality, integrity and availability of data and services; recalls that any software operating in a closed loop remains vulnerable when routine checks are made or when it is updated; considers the TikTok app, owned by Chinese conglomerate ByteDance, to be in breach of the European data privacy framework, making it a potential risk and a source of Chinese-backed disinformation; welcomes the decision of the EU institutions to restrict the use of TikTok on corporate devices; recommends the banning of TikTok at all levels of national government and in the EU institutions;

64. Stresses the need to establish and develop tech alliances with democratic partners to boost strategic autonomy and reduce the EU's dependence on high-risk foreign actors and their technologies as well as to strengthen EU's industrial capabilities in key technological areas, such as artificial intelligence, semiconductors, the cloud and other cutting-edge technologies;

65. Is concerned about the vulnerabilities and increasing attacks on undersea cables and pipelines, pointing in particular to the sabotage of the Nord Stream gas pipeline in September 2022; believes FDI in undersea cables and pipelines creates an additional security risk; welcomes the EU Maritime Security Strategy (EMSA) and asks the Commission to update Parliament on progress to enhance understanding and resilience of subsea infrastructure protection, improve coordination and information sharing, advance monitoring capabilities together with industry, strengthen response mechanisms, and to embed this issue in all aspects of external action;

66. Is concerned about the revelations of how political elites in EU Member States, for example in Germany, have advanced the agenda of Gazprom and expressed constant support for gas supplies from Russia; notes with concern the impact of lobbying efforts by foreign states and corporate actors with an interest in continued production and use of fossil fuels in the EU on policymaking processes; recalls in this regard its findings in the INGE 1 report; welcomes the Commission's REPowerEU proposal to transform the EU's energy system, ending its dependence on Russian fossil fuels; urges EU Member States and the Commission to halt all fossil fuel imports into the EU from autocratic regimes and to move towards sustainable energy sovereignty;

67. Is concerned about the close ties between Hungary and Russia, whereby Russia is exerting its influence through its leverage in the energy sector; regrets that Hungary has not taken significant steps to reduce its energy dependency on Russia; believes more needs to be done to ensure open, strategic autonomy in the energy sector; calls for the deployment of renewable energy to be accelerated, while minimising any further dependency on China;

68. Welcomes the recently proposed critical raw materials act[1]; believes the proposed act is essential to secure European supply chains needed to make the proposed European chips act[2] a success; emphasises the need to continue to seek trade agreements with

[1] Proposal for a regulation establishing a framework for ensuring a secure and sustainable supply of critical raw materials and amending Regulations (EU) 168/2013, (EU) 2018/858, 2018/1724 and (EU) 2019/1020 (COM(2023)0160).

[2] Proposal for a regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act) (COM(2022)0046).

like-minded democracies in securing supply of strategic resources;

Interference during electoral processes

69. Welcomes the work done by the APPF in this regard, especially in preventing and countering prohibited financial payments from non-EU countries into the EU's political system; calls on the Commission and the co-legislators to enhance the APPF's toolbox and to enable the effective tracing of donations to the ultimate payer, thus avoiding the prohibition's being circumvented by the use of intermediaries, in particular by giving the APPF a mandate to obtain information directly from donors' banking institutions as well as by providing a system of push notifications for suspicious transactions from the financial intelligence units in the Member States to the APPF; further calls on the Member States to strengthen legal safeguards preventing that national member parties of European political parties receive payments from non-EU origin at national level, which are then used as contributions for European political parties and foundations; also welcomes the operational contacts the APPF has already established with competent EU institutions and agencies as well as with the Member States to effectively counter attempts to use personal data for electoral purposes; calls on the Member States to further enhance cooperation with the APPF by making specialised contact points available and operational in the competent authorities for data protection and electoral cybersecurity;

70. Welcomes the initiatives taken within the European cooperation network on elections including the joint resilience plans; calls on the Commission to fully involve Parliament in the activities of the network as well as the APPF; considers that similar networks should be established with national parliaments in the Member States; also considers that Member State parliaments and the electoral authorities should do more to inform the public about the risks of interference in national electoral processes; calls on the Commission to draw up a code of good practice on social media applicable to public representatives and authorities, aimed at establishing common standards of conduct, considering that politicians and governments sometimes resort to disinformation to encourage ideological hostility;

71. Notes that the European Parliament has laid down a strategy for the 2024 European elections, which includes a focus on preventing and addressing information manipulation ahead of the elections, without interfering in the political or wider social debates, with full respect for the independence of the mandate of the members; underlines that this strategy should be based on stepping up Parliament's existing measures, including those involving Parliament's task force on disinformation, and therefore calls for the allocation of additional resources to implement the various measures;

72. Stresses the utmost importance of protecting the security, resilience and reliability of the election infrastructure, including, among other things, IT systems, voting machines and equipment, election office networks and procedures, voter registration databases and storage facilities; underlines that information and communication technologies are increasingly prevalent in electoral management and democratic processes; notes that in order to effectively respond to emerging electoral challenges, electoral management bodies need to adopt new working patterns that enhance their ability to prevent risks and demonstrate resilience, also in a complex digital environment; calls for EU Member State and local governments to be provided with a toolkit of services and tools to

combat FIMI; notes that when elections are held, paper ballots should have a verifiable paper trail and be subject to independent audits to ensure the results are accurate; highlights the fundamental role of election observation and independent election monitors;

Covert funding of political activities by foreign actors and donors

73. Reiterates its concerns about the regular revelations of massive Russian funding of political parties and politicians and former politicians and officials in a number of democratic countries in an attempt to interfere and gain leverage in their domestic processes; expresses its concern about Russia's connections with several political parties and politicians in the EU and its wide-ranging interference with secessionist movements in European territories and in the EU, such as in Catalonia where the relevant authorities are urged to carry out a comprehensive investigation and suggests the European Centre of Excellence for Combating Hybrid Threats (Hybrid CoE) in Helsinki conduct a study of this specific case;

74. Takes note that the European cooperation network on elections is mapping foreign funding in EU Member States and expresses its interest in being informed about these efforts; calls for the prohibition of foreign funding from countries outside the EU; calls on the network to identify common EU rules on political campaigning and political party financing, including that from third countries, in particular those standards closing the loopholes identified in the recommendations of the INGE 1 report adopted on 9 March 2022 that would apply to national electoral laws in all Member States, including enforcement mechanisms; calls on the Member States to urgently address the issue of donations from third countries to national political parties, in order to close existing loopholes in their legislation;

75. Takes note of the ongoing legislative negotiations on the statute and funding of European political parties and foundations; expects that these negotiations will enhance the mandate of the APPF in particular in ensuring that financial transactions from non-EU countries into the EU's political system are limited, transparent and subject to stricter controls and will result in an updated framework, which should strengthen the role of EU political parties in the European democratic sphere as well as curb interference by foreign powers; reiterates the need for a balanced and proportionate approach to enable political parties from like-minded third countries, including countries within the Council of Europe, provided they have full rights of representation therein, to participate through membership and contributions, while further enhancing the transparency of funding and decision-making and simultaneously limit the risk of interference by non-democratic foreign entities or high-risk states;

76. Recalls that the APPF should be provided with the necessary resources, in particular human and IT resources, to enable it to fulfil its current tasks and any new tasks provided for by the legislation, which can only be effectively implemented with appropriate additional staff;

77. Takes note of the ongoing legislative work on the transparency and targeting of political advertising; highlights the importance of this proposed regulation that will curb opaque political advertising techniques and stresses the need for co-legislators to adopt it in due time before the European election in 2024; in this regard, recalls its wish to prohibit the purchase of advertisements by actors from outside the EU and the European Economic

Area (EEA) and to guarantee transparency and non-discrimination including via the appropriate labelling with regard to the purchasing of online political advertisements by actors from within the EU; underlines the need for the European political parties to be able to campaign online and EU-wide ahead of the European elections, while limiting the risk of foreign interference;

Cybersecurity and resilience in respect of cyberattacks related to democratic processes

78. Is concerned about the serious increase in cyberattacks, in particular the recent distributed denial-of-service (DDoS) attack against the European Parliament's website on 23 November 2022, for which responsibility was claimed by a pro-Kremlin hacker group and the possible hacking of three MEPs and more than fifty Commission officials with Pegasus software; therefore calls for the resilience and protection capabilities of EU institutions in the digital domain to be strengthened, in particular ahead of the European Parliamentary elections;

79. Welcomes the agreement on the NIS2 Directive and believes it addresses the issue of coordination between Member States; calls on the Member States to ensure enhanced cooperation and to share best practices in the NIS Cooperation Group, especially on cybersecurity for elections; asks for electoral infrastructure to be considered critical infrastructure; believes additional legislation is needed to effectively protect the European ICT supply chain security from risky vendors and protect against cyber-enabled intellectual property theft;

80. Welcomes the Commission's proposal for new rules to establish common cybersecurity and information security across the EUIBAs; welcomes, in accordance with the ECA special report of March 2022, the creation of a new interinstitutional cybersecurity board, the boosting of cybersecurity capabilities, and the promotion of regular maturity assessments and better 'cyber-hygiene'; stresses the need for efficient, timely and close coordination between the EUIBAs through existing structures, such as the Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU) and European Union Agency for Cybersecurity (ENISA); believes these structures should be bolstered and that more efficient coordination is needed; calls on these bodies, agencies and the Commission to regularly inform Parliament about future conclusions and findings concerning cybersecurity and information security in the EU; calls for a complete cybersecurity audit, to determine whether the EUIBAs have sufficient control over the security of their ICT systems and devices, including a risk, vulnerability and threat assessment, backed up with penetration testing, by a leading and verified external third party, when this regulation enters into force and annually thereafter, taking the information security requirements of the institutions into consideration; believes the reported risks and vulnerabilities need to be mitigated in cybersecurity updates, and the recommendations from the assessment should be implemented through the respective cybersecurity policies;

81. Calls on the Commission and ENISA to map existing and planned bodies, agencies and other European organisations working with cybersecurity and to propose solutions to fill potential gaps;

82. Calls on the Council, the Commission and the EEAS to strengthen cyber-related controls on strategic communication channels (e.g. military channels in times of war and CSDP missions);

83. Acknowledges that, when it comes to cyberattacks, prevention is necessary but not sufficient; believes an accurately targeted response is key in countering cyberattacks; believes the EU should tackle cyberattacks by considering the following aspects:

(a) the need for increased responsiveness to and resilience against cyberattacks;

(b) the need for flexibility in critical situations, while upholding the rule of law and fundamental rights;

(c) the need for common regulations to ensure efficient coordination, calls therefore on Member States to speed up implementation of the CER and NIS2 Directives;

(d) the need to share information between and within Member States, in particular with regards to security vulnerabilities, while taking into account the need to hide the critical protection level from public information sharing;

(e) the need for research and investment in new technologies that would increase cyber resilience;

(f) the need to involve actors such as CSOs, the private sector and other partners in a safe and sustainable way;

(g) calls therefore for Member States to adopt a more proactive stance and expand their capabilities in cyberspace based on the 'persistent engagement' and 'defend forward' approaches, in close coordination among Member States and in consultation with the relevant EU counterparts;

The impact of interference on the rights of minorities and other vulnerable groups

84. Recalls that foreign interference is often linked to political objectives contrary to the EU and its democratic values, covering up blatant violations of human rights, restricting the rights of women and LGBTIQ+ communities, and fomenting hatred towards minorities, migrants and the most vulnerable people;

85. Regrets the political instrumentalisation of the migration issue and its use in interference and disinformation campaigns; calls for the efficient management of the EU external border to be ensured in full compliance with fundamental rights;

86. Worries that the LGBTIQ+ community remains a target for foreign interference and disinformation campaigns; is concerned about the situation of the LGBTIQ+ community in several Member States, such as Slovakia, Hungary, and Poland, and the disinformation spread by state-owned media and far-right organisations on the topic; regrets that disinformation and hate-speech against LGBTIQ+ were the primary motive that lead to the murder of two young people in Slovakia in October 2022; calls for the development of long-term programmes supporting local grassroots organisations and citizens' initiatives to help develop the population's resistance to right-wing extremism;

87. Is concerned about the attempts by Russian disinformation to undermine European society's support for Ukrainian refugees; calls on EUIBAs and on national authorities to monitor and debunk Russian disinformation regarding Ukrainian refugees and the war in Ukraine;

88. Calls on the Commission and Member States to strengthen partnerships with NGOs and international organisations working in the field to monitor child labour and slow the spread of disinformation on the matter (e.g. children in armed conflicts);

89. Reiterates its call for a system to make it easy to share material in regional and minority languages; welcomes in this regard the Commission's support to the pilot action entitled 'European Language Equality' (ELE); believes additional measures need to be taken to ensure an effective response to interference targeting minorities; also calls for the EU and the Member States to implement accessible fact-checking in order to combat disinformation and provide access to information in all possible formats for people with disabilities;

90. Reiterates the need for targeted action, through a harmonised EU legal framework, against the spread of disinformation and hate speech on issues related to gender, LGBTIQ+ and Roma people, other minorities, immigrants and refugees and people with disabilities as well as religious communities; reiterates its call on the Commission to develop and implement strategies to hinder the financing of anti-gender groups, movements and individuals that actively spread disinformation or participate in information manipulation targeting LGBTIQ+ people, women's rights, minorities, refugees, people with disabilities and issues affecting them, with the aim of dividing society;

91. Worries that women's rights are being specifically targeted by disinformation, particularly health disinformation, and by foreign interference; calls for a full investigation into the funding sources of gendered disinformation campaigns; reiterates its call for the creation of early warning systems through which gendered disinformation campaigns can be reported and identified;

92. Calls on the Commission and the Member States to develop measures to strengthen independent Russian-language media that are easily accessible to Russian-speaking communities; also calls on the Commission and Member States to support independent commentators in order to counter the influence of third-country propaganda on minorities in Europe;

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

93. Denounces in the strongest terms the alleged attempts by foreign countries, including Qatar and Morocco to influence Members, former Members and staff of the European Parliament through acts of corruption, which constitute serious foreign interference in the EU's democratic processes; underlines the need to step up efforts to enhance the transparency and integrity of the EU institutions, and to combat corruption, manipulation, influence and interference campaigns; reiterates its call for updated transparency rules and ethics, mapping foreign funding for EU-related lobbying, including funding for non-profit organisations and proper regulation and monitoring of friendship groups; reiterates the need to immediately suspend all work on legislative files relating to Qatar and Morocco, as well as for the access badges of representatives of interests of both countries, until the judicial investigations provide relevant information and clarification and evaluate which dossiers may have been compromised as a result of this foreign interference;

94. Welcomes the extension of the term of office and updated mandate for the ING2, special committee and expects the ING2 committee to prepare an impactful report identifying the flaws in the European Parliament's rules on transparency, ethics, integrity and corruption and to make proposals for the reforms to effectively fight corruption and other means used by foreign actors to influence European decision-making processes, considering that any potential enhanced disclosure requirements should be weighed against the need to protect certain vulnerable individuals and groups;

95. Regrets that the recommendations from the INGE 1 report on introducing more stringent transparency rules, mapping of foreign funding for EU-related lobbying, and ensuring it is entered in the records to allow for the identification of funding from foreign governments, have not yet been implemented;

96. Recalls the commitments made by the President of the Commission during her State of the Union address regarding the need to update the EU legislative framework for combating corruption; considers that such an update should target in particular the issue of the capture of elites by foreign interests, revolving doors and trafficking in influence in order to prevent foreign agents from interfering the EU political system; invites also the Commission to tighten its rules to prevent such capture by autocratic or high-risk governments or entities under their control, to deal with the issue of elite capture in the annual rule of law reports; recalls Parliament's repeated calls for the establishment of a new permanent sanctions regime dedicated to targeting individuals and entities responsible for large-scale corruption;

97. Takes note of the judgment of 22 November 2022 of the Court of Justice of the European Union in case C-37/2013 [1], invalidating a provision of the fifth Anti-Money Laundering Directive[2], whereby Member States had to ensure that information on the beneficial ownership of companies should be accessible in all cases to any member of the general public; stresses that registers of beneficial ownership information are an essential tool for civil society organisations, researchers, investigators and journalists to detect alleged corruption and illicit business interests, and that restricting access to those registers severely limits future monitoring of true ownership by the general public; considers that this invalidation constrains the work of a wide range of professionals fighting corruption and money laundering; calls on the Commission to find proper ways to ensure that information on the beneficial ownership of companies is accessible to the general public; calls on the Commission to propose measures under the Anti-Money Laundering Directive with a view to limiting the use of cash so as to discourage the use of illegitimate money and thereby preventing corruption; regrets that some Member States have taken the judgment as a pretext to suspend access to the register outright;

98. Is of the opinion that the data on foreign influence through interest representatives at the EU level should be widely available and clearly presented; welcomes the changes introduced by the interinstitutional agreement of 20 May 2021 on a mandatory

---

[1] Judgment of 22 November 2022, Luxembourg Business Registers , C-37/20, ECLI:EU:C:2022:912.

[2] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (OJ L 156, 19.6.2018, p. 43).

transparency register[1] in this regard; recommends, however, that a specific foreign influence section be inserted in the EU Transparency Register or that a foreign influence register be established; considers that the EU Transparency Register should include a list of high-risk countries; recommends stronger requirements and incentives for foreign powers to register; considers enhanced registration and disclosure requirements to be necessary for CSOs, consultancies, agencies, foundations, think tanks and private companies receiving foreign funding;

99. Calls on the Secretariat of the EU Transparency Register to ban any entities with direct or indirect relations with the Government of Russia, pursuant to the Council decision of 3 June 2022 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine[2]; calls on the same measures to be applied to Belarus;

100. Reiterates its concerns about partnerships between universities and Chinese entities, including Confucius Institutes, but especially those research facilities related to the Chinese military complex, and the risk they may pose to academic freedom and protection of intellectual property; is alarmed at recent findings[3] that a considerable number of European researchers working on artificial intelligence, quantum technologies, integrated circuits, space research, new materials research, neuroscience and biotechnology are being directly funded by the People's Republic of China; reiterates its call on Member States' authorities and research institutes to review those partnerships, and, where alleged espionage or interference is substantiated, take action to enforce and safeguard European economic and political sovereignty, including through denial of funding or revocation of licences of associated institutes; reiterates that academic freedom is a fundamental value in any democratic society; urges Member States to make better use of existing mechanisms to protect scientific, industrial and technical knowledge, and to extend them to the humanities and social sciences; calls for more transparency in the funding of research activities and the financial support they receive, notably through the establishment of due diligence procedures to assess whether the foreign funding of projects pose a security threat;

101. Highlights that China is trying to combine civilian and military scientific research within the framework of the civil-military integration programme; demands the immediate termination of existing cooperation with research institutions that are directly funded by the Chinese military or have ties with it, and to take stock of what scientific knowledge might have gone to the Chinese side; welcomes the publication of the guidelines on tackling R&I foreign interference by the European Commission, but suggests proportionate measures be applied to academic and research institutions, and that more transparency be ensured in foreign partnerships; expresses concern about the Chinese National Intelligence Law, which requires Chinese researchers at Western universities to share their knowledge with the state, and about China's reliance on spying as a means of obtaining knowledge to further its economic and military goals;

---

1 Interinstitutional Agreement of 20 May 2021 between the European Parliament, the Council of the European Union and the European Commission on a mandatory transparency register (OJ L 207, 11.6.2021, p. 1).

2 Council Decision (CFSP) 2022/884 of 3 June 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine (OJ L 153, 3.6.2022, p. 128).

3 Study entitled 'How to Do Trusted Research: China-Specific Guidelines for European Stakeholders', published in September 2022.

calls for mandatory commitments to greater diligence and compliance in academic cooperation with Chinese universities and researchers, and for any cooperation with Chinese universities to be subject to a comprehensive security risk assessment;

102. Expresses concerns about the ongoing activities of Russkiy Dom (Russian House) offices funded by the EU-sanctioned Russian federal agency Rossotrudnichestvo, whose misleading projects spread disinformation, propaganda and the Kremlin's agenda among EU civil society;

103. Welcomes the publication by the Commission of a toolkit on how to mitigate foreign interference in research and innovation in order to help European universities and research organisations to detect and prevent foreign interference while remaining open to partnerships; calls on the Commission to include academic and research institutions in the Defence of Democracy Package; calls on the Commission and Members States to further coordinate actions in this field, in particular to step up the role of ethics and security officers in higher education institutions; calls on the Commission to further develop guidelines for trusted research and knowledge security in order to support the integrity of international research collaboration with European organisations; highlights the potential in a register or database of possible sleeping or foreign agents from high-risk states at European universities and research organisations;

104. Expresses concerns over recent reports about the establishment of Chinese overseas police stations within the EU; calls on the Member States and EU authorities to investigate the alleged existence of these police stations and to take coordinated action against any illegal activities associated with China's United Front Work Department in Europe; reiterates that such stations constitute a threat to the national security of the Member States concerned and of the Union in general, and should therefore be prohibited; calls on the Member States to close them down immediately; condemns the practice of threatening people living in the European Union, in particular the Chinese diaspora and political dissident groups, as well as the imprisonment of their relatives in China in order to coerce persons living abroad into returning to China;

105. Is concerned about the allegations of illegal police operations on foreign soil eschewing official bilateral police and judicial cooperation; calls on the Commission to examine the so-called Chinese overseas police service stations inside the EU, which allegedly have persuaded thousands of suspected fugitives to return to China, and to take the appropriate steps in this regard; demands the Chinese authorities and Chinese embassies in EU Member States to adhere to standard international procedures;

106. Denounces signs of Turkish interference and persecution of political activists, opposition leaders and minorities within the EU; condemns Türkiye's new Disinformation Law proposal, which poses a threat to the freedom of speech in the country;

107. Deplores the dissemination of disinformation and the oppressive use of the internet by the Iranian regime to conceal gross human rights violations, violence against protestors and abuses of power; is worried by the interference of Islamist organisations inspired by foreign states;

108. Is concerned about the growing influence activities of foreign authoritarian state intelligence agencies within the EU, especially in Brussels; reiterates its call on national

authorities to review and update their anti-espionage frameworks; in this regard, welcomes the Belgian government's announced modernisation of the anti-espionage framework and calls for more capacity for the EU Intelligence and Situation Centre (INTCEN) to carry out its counterintelligence mandate and deepen cooperation with national authorities; calls on immigration authorities to be more vigilant when screening the staff of foreign companies, such as TASS and COSCO, from high-risk countries, when they apply for work visas; furthermore, calls on immigration authorities to enhance coordination to make travel by foreign intelligence officers using false identities more difficult;

109. Expresses concern about a recent New York Times investigation accusing the Russian Imperial Movement, a supremacist group, of having organised a campaign to send letter bombs to prominent Spanish citizens in late 2022, with the help of the GRU, the Russian military intelligence service; warns of the risk of espionage in French airports such as Strasbourg, Bordeaux, Brest, Quimper and Toulouse, which use the Chinese equipment company Nuctech, linked to the Chinese regime and its military-industrial complex, for baggage screening; underlines that Nuctech is present in 26 of the 27 EU Member States, and recalls that Lithuania, the United States and Canada have banned the company from their public contracts;

110. Calls on EU political parties to develop a strong response to hate speech and harassment campaigns against Members of Parliament; calls on Parliament's administration to develop an institutionalised procedure to be put in place when such campaigns against elected EU representatives occur;

Deterrence, attribution and collective countermeasures, including sanctions

111. Welcomes the EU-wide sanctions and the capacity of EU decision-makers to act quickly to temporarily restrict the broadcasting of certain propaganda channels following Russia's unjustified and illegal war of aggression against Ukraine and underlines the need to ensure consistent implementation and non-circumvention of those sanctions; welcomes the alignment of certain EU candidate and potential candidate countries with these measures; calls on the Commission to cooperate more closely with Member States on imposing and implementing sanctions; welcomes the General Court's judgment of 27 July 2022 in case T-125/22 RT France[1] , in which the Court rejected RT's argument that the prohibition of broadcasting is illegal, and therefore upheld the prohibition of broadcasting content imposed on RT France; calls on the Commission and the Council to include satellite broadcasting in the sanctions packages against Russia, the GRU affiliated 'news agency' InfoRos, as stated in its May 2022 resolution[2] and to include all prominent Kremlin propagandists on EU lists of sanctioned individuals; regrets that these channels are still able to spread their narratives under false aliases or through other channels in the European Union; especially strongly condemns the opening of an RT (formerly Russia Today) office in Belgrade and the launch of its online news service in Serbian, thus allowing this malign actor to spread its disinformation in the whole region; urges, in this context, the Serbian authorities to align with the Council's decision on the suspension of the broadcasting activities of

[1] Judgment of 27 July 2022, RT France v Council, T-125/22, ECLI:EU:T:2022:483.

[2] European Parliament resolution of 19 May 2022 on the social and economic consequences for the EU of the Russian war in Ukraine — reinforcing the EU's capacity to act (OJ C 479, 16.12.2022, p. 75).

Sputnik and RT;

112. Welcomes the Commission's proposal for a directive on the definition of criminal offences and penalties for the violation of Union restrictive measures (COM(2022)0684) and calls on the Commission to assess the possibility of the European Public Prosecutor's Office being tasked with ensuring the consistent and uniform investigation and prosecution of such crimes throughout the EU; calls for the EU INTCEN to be given greater resources to help inform on and enforce EU sanctions, as well as to improve the exchange of forensic information and coordinate attribution policy more effectively;

113. Expresses its concerns about the rise in the manipulation of automatic identification systems (AIS) to subvert the GPS data and manipulate the position of vessels, allowing certain actors to circumvent sanctions; calls on the Commission to impose stricter AIS security protocols and calls for the inclusion of AIS spoofing technology within the EU dual-use export control regime;

114. Reiterates its call to impose costs on perpetrators of foreign interference by means of a strong attribution capacity; takes note of the ongoing reflection based on the Council conclusions of June 2022 regarding the preparation of a toolbox to complement the EU Hybrid Toolbox and Cyber Toolbox, specifically addressing activities involving FIMI; notes that the FIMI toolbox was expected to be introduced in the autumn of 2022; strongly believes this toolbox should include a specific sanctions regime on FIMI as well as measures to strengthen the attribution capacity of European institutions and national governments; notes that these measures should include guidelines for national sanctions against FIMI and be applied by the Member States acting in a coordinated way; calls on Member States to discuss the possibility of qualified majority voting when sanctioning high-risk states; notes that the added value of the Hybrid Toolbox and the proposed FIMI Toolbox, compared to the Cyber Toolbox, will reside in the agreement of norms of responsible state behaviour that offer an enhanced interpretation of what constitutes a violation of the principles of international law, such as sovereignty and non-interference in the internal affairs of a Member State;

115. Reiterates the importance of the EU's ability to defend itself from disinformation attacks and to counteract foreign interference; calls in that regard for sufficient funding and for possible investment and legislative gaps to be addressed; calls on the Members States to update, if necessary, their legal frameworks to introduce a legal basis on which to penalise foreign interference from high-risk countries; welcomes the introduction of such a legal basis into Belgium's draft penal code, which will allow for the better protection of the European institutions on its territory;

116. Calls on Member States and the Commission to consider how to counter disinformation from individual actors inside the EU, such as influencers on social media or politicians promoting disinformation on behalf of high-risk states, etc.; highlights the potential need to develop a sanctions regime against perpetrators engaging in FIMI inside the EU;

Neighbourhood, global cooperation, multilateralism

117. Is concerned about attempts by Russia to manipulate the discourse around global food and energy security, which have been echoed in other communication channels, including mainly Chinese outlets and in some instances Al Jazeera, blaming the West

for the surge in food prices due to its sanctions on Russia; emphasises that these manipulated narratives have gained considerable traction, primarily in the Global South and in some candidate and potential candidate countries; recalls that Russia is solely responsible for the disruption of Ukraine's agricultural production and trade as a result of its war of aggression against the country; calls on the EEAS, therefore, to take additional measures to counter the dissemination of manipulated narratives in the Global South, spread by Russia and China, including by strengthening the tools and resources of its StratCom division and its CSDP/CFSP missions and operations, and through increased cooperation and coordination with the United States and other like-minded partners; believes the EU should work closely with Ukraine in countering manipulated narratives coming from Russia; calls for the EU institutions, therefore, to provide support to Ukraine's diplomatic outreach in the Global South; calls for closer cooperation with regional organisations from the Global South, such as the African Union and ASEAN, to exchange best practices for countering FIMI;

118. Recalls that many information manipulation campaigns and much state-sponsored propaganda target countries making strategic choices about their democratic reform processes and the pro-European orientation of their countries; underlines the importance of proactive, effective and transparent communication, and calls for closer cooperation on strategic communication with partner organisations and countries to counter FIMI in accession countries and strategically important areas such as the Western Balkans and Eastern Partnership countries; believes that the EU should engage more with the US in relation to neighbouring countries in order to build resilient democratic societies; recalls that the stability of these countries is a matter of peace and security;

119. Calls therefore for strategic and proactive measures to counter hybrid threats and to prevent third-country interference in the political, electoral and other democratic processes of accession countries; calls for efforts to increase the resilience of these countries against FIMI campaigns and encourage candidate and potential candidate countries to take decisive steps to tackle manipulative disinformation, malign propaganda and other hybrid threats;

120. Regrets the lack of progress made in and the continuing slow pace of the enlargement process in the Western Balkans, which has led to a drop in support for the EU and frustration among the population of the region; condemns the continuation of Russian attempts to exert influence over the Western Balkans, which has to be understood as part of a broader strategy to promote authoritarianism in Europe; observes, further, that the pro-Russian message is being spread through Serbian and Hungarian-owned media in the Western Balkans; is concerned about recent findings that Serbia is the country most vulnerable to malign foreign influence in the Western Balkans, particularly from Russia and China, and that Serbia still has not implemented sanctions against Russia and has not aligned to the EU's foreign policy;

121. Calls on the Commission in its upcoming evaluation of the GDPR to provide clarity regarding whether and how the GDPR impacts data sharing to combat information manipulation between public, private and academic actors in the EU and in cooperation with like-minded partners;

122. Believes the Global Gateway strategy will be an important geopolitical tool in intensifying the EU's engagement and relations with partners from the Global South, responding to China's influence, through its Belt and Road Initiative, and that of other

non-EU countries such as Russia and Iran, building trust with non-EU countries and bolstering trust among candidate countries to strengthen the image of the EU vis-à-vis Russia and China; believes it should be approached as a geopolitical project that makes strategic investments on the basis of Europe's needs for the digital and green transition, through a strong connection with the Critical Raw Materials Act and Chips Act, and asks for the Commission to provide clarity on the priorities of the Global Gateway initiative; believes it is of the utmost importance to act as 'Team Europe' in implementing the strategy, ensure proper democratic scrutiny, the full involvement of Parliament and coordinated action between all EU institutions and Member States, as well as with the European private sector; calls on the Commission and the EEAS to closely cooperate and coordinate with other connectivity initiatives involving like-minded partners, such as the US, Japan, South Korea and Taiwan, to ensure fundamental rights are safeguarded;

123. Strongly supports the work done by the EEAS Strategic Communication, Task Forces and Information Analysis division and its geographical task forces; believes more attention needs to be paid to outlining the threat landscape in the context of actors related to the Chinese authorities, as well as in the EU's Eastern and Southern Neighbourhoods and beyond; welcomes, against this background, the EEAS' work on enhancing the capacities of the EU delegations and CSDP missions and operations to respond to FIMI, in close cooperation with international partners; believes, however, that more resources should be allocated to strengthening their work, both within the EEAS headquarters and in the field; calls for further capacity-building, including tailored training for CSDP personnel, increased knowledge sharing and coordination with other EU missions, operations and delegations, better engagement with local media and society and proactive and reactive communication in local languages;

124. Welcomes the cooperation mechanisms in place with the US, such as the ongoing EU-US cooperation within the Trade and Technology Council (TTC); notes with interest the joint statement following the TTC of 5 December 2022 stating in particular that working group 5 on Data Governance and Technology Platforms and working group 6 on the Misuse of Technology Threatening Security and Human Rights 'are coordinating to understand and address the spread of Russian information manipulation and interference, particularly in the context of Russia's aggression against Ukraine, and its impact on non-EU countries, notably in Africa and Latin-America'; welcomes the Commission's commitment to regularly inform Parliament on the work of the TTC and calls for continuing efforts to address common challenges in these areas; in addition, calls on the Commission and EEAS to further intensify the work with the US on sharing best practices and operational knowledge, as well as on the development of common definitions and approaches;

125. Considers initiatives such as the TTC and the G7 Rapid Response Mechanism (RRM), to be important platforms of cooperation between like-minded partners in developing tools and sharing best practices to counter FIMI; calls on the EU to take the lead in these cooperation initiatives to ensure global standards are being developed in accordance with European values; calls on the Commission and EEAS to regularly include Parliament, through its administration, in discussions with like-minded partners and identify areas where Parliament's support could add value to the process; calls for deeper cooperation between democratic partners, such as the US, and promotion of academic cooperation in order to avoid a situation whereby China dominates the development of AI;

126. Calls for strengthened and direct contact between specialised parliamentary committees in transatlantic relations through the Transatlantic Legislators' Dialogue;

127. Welcomes the UN's Global Code of Conduct; urges the EEAS to remain closely involved in the process and to appeal to other UN member states on the importance of common awareness of the global challenges and the need for intensive cooperation; believes the Code should not focus solely on platforms, but also look at other state and non-state actors; calls on platforms to allocate more resources and capacity to monitoring harmful content in local languages or dialects; calls on platforms to include approaches to mitigate the risks from AI and other technologies; reiterates the need to safeguard fundamental rights within the Code; believes a change in international law will be extremely difficult to make and therefore suggests the EU work closely with like-minded partners to develop international responses to FIMI;

128. Is concerned about the safeguarding of fundamental rights in the UN process of drafting a Global convention on cybercrime; calls on the Commission and EEAS to ensure European norms, rights and values are upheld in the process, including by promoting the Budapest Convention as the global standard; recalls the danger of processes to fight against disinformation being used as a pretext to curb media freedom;

129. Recalls that all efforts to counter foreign interference should do their utmost to respect CSOs, existing rulings by the European Court of Human Rights and the European Court of Justice as well as the EU Charter for Fundamental Rights, and should not be abused to justify and legitimise restrictive policies, which is a concern that also extends to EU Member States; calls for criteria to suspend or revoke agreements with non-EU countries to be applied more rigorously, for example in the event of human rights violations, as the current application of those criteria exposes the EU to foreign influence;

130. Condemns the attempts of private military companies (PMCs), such as the Wagner Group and other armed groups, militias and proxies, including as the Kadyrovites and the Night Wolves, to influence democratic processes in several countries across the world; condemns recent threat and intimidation messages sent by the Wagner Group to the European Parliament; calls on the Council and the Member States to include Russian PMCs on the EU's terrorist list; calls on the EEAS to create an initiative with like-minded partners to counter malign non-state actor groups, such as Wagner; emphasises that the existing EU toolboxes should include responses, such as sanctions, to non-EU states financing or cooperating with private military companies in vulnerable regions;

131. Highlights the importance of close and continuous cooperation with the Eastern Partnership countries, notably Ukraine and other candidate countries, in building resilience against hybrid attacks; believes that this potential cooperation could take the form of an 'Information Ramstein', mirroring the Ramstein Defence Contact Group, which would bring together media experts from Ukraine, the EU and beyond to discuss the lessons learnt from Ukrainian resilience against Russian information warfare and to develop joint operations; encourages the EU and its Member States furthermore to deepen cooperation with Taiwan in countering disinformation campaigns and interference operations;

132. Calls on the Commission and the EEAS to increase cooperation with other like-minded

partners on developing mechanisms to address election interference, for example with the electoral authorities of Taiwan, Canada, Australia and Brazil; calls for increased cooperation with NATO in building resilience among EU and NATO Member States; calls for EU delegations and Member States' embassies in third countries to constantly monitor and map disinformation techniques and actors in the respective countries where they are based, for which they should receive the necessary resources, and to help partner countries in developing and strengthening their critical electoral infrastructures, and to set ambitious standards that offer enhanced interpretation of existing international law; considers it necessary to carry out updated training for EU officials and diplomats concerning FIMI;

133. Reiterates its recommendation to establish regional strategic communication hubs outside the EU, initiated by the EEAS and with sufficient funding; believes that these multi-lingual hubs should strengthen the EU's voice in the priority regions (i.e. the Western Balkans, the Indo-Pacific, the Middle East and North Africa (MENA), Latin America, and Western and Eastern Africa), improve its outreach to regional media and rebut foreign sponsored information manipulation and disinformation campaigns targeting EU values and interests; underlines that the activities of the hubs should also provide support to EU delegations and Member States' diplomatic missions, offer synergies with the EU media service providers present in these regions and prioritise engagement with local media and opinion influencers;

134. Calls on the EEAS and the Member States to keep working closely with like-minded partners in establishing common norms of responsible state behaviour and definitions, and developing tools and legislation to counter foreign information manipulation and interference; calls on the EEAS to strengthen multilateral and multi-stakeholder cooperation with non-EU countries, civil society and industry on countering FIMI through like-minded partnerships and in international diplomatic dialogues and forums while ensuring the safeguarding of fundamental rights when developing tools to counter FIMI; regrets that some EU Member States still have not filled the vacant national expert positions within the EU Hybrid Centre of Excellence (Hybrid CoE); calls on Member States to appoint national representatives and experts to the Hybrid CoE;

135. Underlines the importance of parliamentary diplomacy and missions to amplify the EU's debunking efforts and strategic interests, and communicate effectively with non-EU countries, especially in Africa and the MENA region; underlines the great value of the initiatives taken by Parliament and its services in supporting parliamentary democracy in non-EU countries by reinforcing the democratic functioning of parliaments, parliamentary mediation and dialogue, observing elections and engaging in debates with civil society;

136. Highlights the potential for the EU to contribute to establishing a global community of fact-checkers and global quality standards for fact-checking inspired by the European Code of Standards for Independent Fact-Checking Organisations; considers it necessary, furthermore, for the EU to support fact-checking efforts in candidate and enlargement countries;

137. Welcomes the support channelled through the European Endowment for Democracy, but believes more action needs to be taken by the EU to support independent journalism in areas influenced by malign foreign actors, such as Russia and China, as well as to provide strategic support and structural funding for local NGOs, CSOs, fact-checkers

and media based outside the EU, including in high-risk countries, enlargement and candidate countries; reiterates its call, therefore, to establish a specific European democratic media fund to support journalism in enlargement and EU Neighbourhood and candidate countries; notes that many journalists from Ukraine have come to the EU together with the growing number of war refugees and calls for tailored support for the Ukrainian media environment, which has been severely harmed by the Russian invasion; calls on the EEAS to include a parliamentary dimension in its outreach and capacity-building initiatives in EU neighbourhood countries to support CSOs and the independent media;

138. Considers that the EU has become a major hub for independent newsrooms from Russia and Belarus, since these countries have eradicated independent media inside their territories; believes that independent media can contribute to countering disinformation spread by the Kremlin and in the long term to shaping Russia as a more democratic country at peace with its neighbours; asks the Commission therefore to develop a long-term structured approach including the establishment of a sufficiently funded policy that would provide long term core support for independent Russian and Belarusian media and journalism in exile;

139. Calls on the Commission and the EEAS to move away from a country-agnostic approach towards a risk-based approach and to not shy away from identifying and naming at international forums, such as the UN, those countries that have attempted to conduct foreign interference, in order to make other countries aware of the risks posed by the issue;

140. Instructs its President to forward this resolution to the Council and the Commission.

Follow us

Published by:	**EPP Group in the European Parliament**
Directorate Campaigns:	**Events Unit** **Publications and Programmes**
Editor:	**Marek Evison**
Responsible:	**Fiona Kearns**
Coordinator:	**Daniela Steiner**
Address:	**European Parliament,** **60 Rue Wiertz,** **B-1047 Brussels**
Internet:	**www.eppgroup.eu**
E-mail:	**epp-publications@ep.europa.eu**
Copyright:	**EPP Group in the European Parliament**
Published:	**December 2023**