European Parliament
2019-2024

Plenary sitting

A9-0187/2023

15.5.2023

REPORT

on foreign interference in all democratic processes in the European Union, including disinformation
(2022/2075(INI))

Special Committee on foreign interference in all democratic processes in the European Union, including disinformation (INGE 2)

Rapporteur: Sandra Kalniete

PR_INI

CONTENTS

Page

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

on foreign interference in all democratic processes in the European Union, including disinformation
(2022/2075(INI))

The European Parliament

– having regard to its resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation[1] (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[2],

– 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 in Europe[3],

– 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[4],

– having regard to its resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third countries[5],

– 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

[1] OJ C 347, 9.9.2022, p. 61.
[2] Texts adopted, P9_TA(2022)0406.
[3] OJ C 347, 9.9.2022, p. 2.
[4] Texts adopted, P9_TA(2022)0448.
[5] OJ C 224, 27.6.2018, p. 58.

after the EP report on EU strategic communication to counteract propaganda against it by third countries[6],

– 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’[7],–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[8],

– 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 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)[9],

– 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[10] (CER Directive);

[6] OJ C 23, 21.1.2021, p. 152.
[7] OJ C 184, 5.5.2022, p. 71.
[8] OJ L 156, 5.5.2021, p. 1.
[9] OJ L 277, 27.10.2022, p. 1.
[10] OJ L 333, 27.12.2022, p. 164.

– 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[11],

– 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[12],

– 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,

– 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 Rule 54 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

[11] Texts adopted, P9_TA(2023)0027.
[12] OJ L 207, 11.6.2021, p. 1.

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 Turkey; 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)[13] 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 engineers and data scientists dedicated to the study of algorithms;

[13] 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.

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[14]; 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[15]; 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) cooperation group; whereas the European Court of Auditors has concluded that since

[14] 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.
[15] 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).

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 Belgian national Olivier Vandecasteele, 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) 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 2015/8499[16], 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 activities, (d) consistent violation of human rights, (e) revisionist policy towards the existing international legal order, (f) enforcement of authoritarian ideology

[16] 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 (OJ L 141, 5.6.2015, p. 73).

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 President Věra Jourová's public call in Tallinn in January 2023[17] 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 of the Treaty on the Functioning of the European Union 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 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;

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

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[18], 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[19] (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 EU and that may present a risk to public security; recommends that the countries of the

[18] 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).
[19] 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).

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[20] (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

[20] 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).

flag specific content; calls on platforms to prioritise fact-based information coming 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[21]; 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

[21] 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 791, 21.3.2918, p. 1).

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; 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[22]; believes the proposed act is essential to secure European supply chains needed to make the proposed European chips act[23] a success; emphasises the need to continue to seek trade agreements with 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

[22] 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).
[23] Proposal for a regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act) (COM(2022)0046).

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 calls on the European Centre of Excellence for Combating Hybrid Threats (Hybrid CoE) in Helsinki to 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[24], invalidating a provision of the fifth Anti-Money Laundering Directive[25], 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 transparency register[26] 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[27]; 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[28] 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

[24] Judgment of 22 November 2022, *Luxembourg Business Registers*, C-37/20, ECLI:EU:C:2022:912.
[25] 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).
[26] 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).
[27] 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).
[28] Study entitled 'How to Do Trusted Research: China-Specific Guidelines for European Stakeholders', published in September 2022.

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; 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[29], 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[30] 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 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

[29] Judgment of 27 July 2022, RT France v Council, T-125/22, ECLI:EU:T:2022:483.
[30] 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).

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.

EXPLANATORY STATEMENT

Background

Malicious foreign actors use information manipulation and other tactics to interfere in democratic processes and they aim to weaken the democratic governance of the targeted countries.

Foreign interference, disinformation, and numerous attacks on and threats against democracy are expected to continue in ever-greater numbers and more sophisticated ways in the run-up to the European Parliament elections in 2024.

Special Committee INGE 1

Therefore, the European Parliament stepped up in its role against foreign interference and disinformation: Following the European Parliament's Decision of 18 June 2020, the first Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE 1), was established. The Special Committee was tasked to draw up a report containing factual findings and recommendations concerning the measures and initiatives to be taken in countering foreign interference and disinformation.

After eighteen months of work – characterised by 50 hearings with over 130 invitees, including 5 Commissioners (Věra Jourová, Vice-President of the Commission, Values and Transparency; Margaritis Schinas, Vice-President of the Commission, Promoting our European Way of Life; Thierry Breton, Commissioner for Internal Market; Josep Borrell, Vice-President of the European Commission/High Representative of the Union for Foreign Affairs and Security Policy; and with Margrethe Vestager, Executive Vice-President for A Europe Fit for the Digital Age and Competition), experts, journalists, representatives from think tanks, as well as representatives from Google, Facebook, YouTube, Twitter, two Facebook whistle-blowers and a Nobel Peace Prize laureate – the Resolution of the first Special Committee on Foreign Interference in all Democratic Processes of the European Union, including Disinformation was adopted on 9 March 2022, only a few days after the Russian Federation's unprovoked and unjustified military aggression against Ukraine began.

The Resolution 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, covert political funding as well as elite capture and co-optation. It provided both, the diagnosis of the EU's vulnerabilities and recommendations for strengthening the EU's resilience.

Special Committee INGE 2

Following the European Parliament's Decision of 10 March 2022, it set up INGE 2, a new Special Committee with a revised mandate. The new Special Committee INGE 2 was vested with the responsibilities to follow up on the implementation of the INGE 1 Resolution, and to engage in a dialogue with policy makers on the national, the European and the international level in order to contribute to the overall institutional resilience against foreign interference,

hybrid threats and disinformation in the run-up to European elections in 2024. Since its constitutive meeting on 12 May 2022, ING2 focused particularly on Russian and Chines interference, for instance in Ukraine, and in the distinct cases of Hungary and Spain (Catalonia); on the African continent or in enlargement countries, including Western Balkans. It looked as well into elite capture and revolving doors politics, and into intimidation attempts against Members of the European Parliament by foreign actors. It held an exchange of views with Intelligence Services of EU Member States and with parliamentary bodies deputed to survey and oversee the activities of these services.

All committee meetings were organised in cooperation with standing parliamentary committees and delegations, for instance with the Committee on the Internal Market and Consumer Protection (IMCO), the Committee on Culture and Education (CULT) and the Committee on Civil Liberties, Justice and Home Affairs (LIBE), the Committee on Foreign Affairs (AFET), the Subcommittee on Security and Defence (SEDE), the Committee on Development (DEVE) and the Delegation to the ACP-EU Joint Parliamentary Assembly (DACP), the Delegation to the EU-Russia Parliamentary Cooperation Committee (D-RU), the Delegation for Relations with the People's Republic of China (D-CN).

Since May 2022, ING2 invited as many as two dozen experts and policy makers including Věra Jourová, Vice-President for the Values and Transparency, Commission; Josep Borrell, Vice-President of the European Commission/High Representative of the Union for Foreign Affairs and Security Policy; Audrey Tang, Minister of Digital Affairs of Taiwan; or Liubov Tsybulska, Founder of the Centre for Strategic Communications and Information Security under the Ministry of Culture and Information Policy of Ukraine.

Finally, in order to best focus on institutional and legislative resilience building in the run-up to European elections in 2024, ING2 established a close cooperation with NATO StratCom in Riga (Latvia), the Hybrid CoE in Helsinki (Finland), with the Australian government and authorities and respective bodies at the UN in New York.

Hence, the work of the second Special Committee follows seamlessly from the first, and the present INGE 2 Resolution is to be complementary to the INGE 1. It therefore includes recommendations and updates on the EU's coordinated strategy against foreign interference; on EU resilience building; on interference using online platforms; on the critical infrastructure and strategic sectors; on interference during electoral processes; on covert funding of political activities by foreign actors and donors; on cybersecurity and resilience of democratic processes; on the impact of interference on the rights of minorities and other vulnerable groups; on deterrence, attribution and collective countermeasures, including sanctions; and on neighbourhood policy, global cooperation, and multilateralism.

MINORITY REPORT TABLED BY CLARE DALY ON BEHALF OF THE GROUP OF THE LEFT

Attempts by external actors to subvert democratic processes in Europe are real and require attention, but should not be exaggerated and cannot justify a departure from the rule of law, respect for fundamental rights or political freedoms.

This report is symptomatic of deepening authoritarianism and national security overreach on the part of ruling class parties within the EU. It views the operation of democratic society through a paranoid lens, where the exercise of political freedoms across every domain of life in Europe is regarded as a potential source of ever-multiplying "foreign" threats.

Among the repressive measures it contemplates are a regime of delegated, pro-active mass censorship by privately-owned tech platforms ("content moderation"), enhanced EU propaganda capabilities ("strategic communication"), the invention of a new crime of "foreign interference," and the use of sanctions against persons and entities accused of disinformation, including within the EU.

Such measures likely breach EU fundamental rights obligations. If introduced, they will be abused. Their wider effects will include erosion of rule of law, a contraction of the civic space, and a chilling effect on the exercise of democratic rights. They have no place in a free and democratic society.

INFORMATION ON ADOPTION IN COMMITTEE RESPONSIBLE

Date adopted	26.4.2023
Result of final vote	+: 27 –: 1 0: 1
Members present for the final vote	Aurélia Beigneux, Vladimír Bilčík, Ioan-Rareş Bogdan, Anna Bonfrisco, Mercedes Bresso, Włodzimierz Cimoszewicz, Clare Daly, Anna Júlia Donáth, Daniel Freund, Raphaël Glucksmann, Sandra Kalniete, Andrey Kovatchev, Nathalie Loiseau, Morten Løkkegaard, Benoît Lutgen, Lukas Mandl, Radka Maxová, Maite Pagazaurtundúa, Nacho Sánchez Amor, Andreas Schieder, Sabine Verheyen, Viola von Cramon-Taubadel, Javier Zarzalejos
Substitutes present for the final vote	Reinhard Bütikofer, Laura Ferrara, Sandro Gozi, Pirkko Ruohonen-Lerner, Isabel Wiseler-Lima
Substitutes under Rule 209(7) present for the final vote	Grzegorz Tobiszowski

FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE

27	+
ECR	Pirkko Ruohonen-Lerner, Grzegorz Tobiszowski
ID	Anna Bonfrisco
NI	Laura Ferrara
PPE	Vladimír Bilčík, Ioan-Rareş Bogdan, Sandra Kalniete, Andrey Kovatchev, Benoît Lutgen, Lukas Mandl, Sabine Verheyen, Isabel Wiseler-Lima, Javier Zarzalejos
Renew	Anna Júlia Donáth, Sandro Gozi, Nathalie Loiseau, Morten Løkkegaard, Maite Pagazaurtundúa
S&D	Mercedes Bresso, Włodzimierz Cimoszewicz, Raphaël Glucksmann, Radka Maxová, Nacho Sánchez Amor, Andreas Schieder
Verts/ALE	Reinhard Bütikofer, Daniel Freund, Viola von Cramon-Taubadel

1	-
The Left	Clare Daly

1	0
ID	Aurélia Beigneux

Key to symbols:
+ : in favour
- : against
0 : abstention