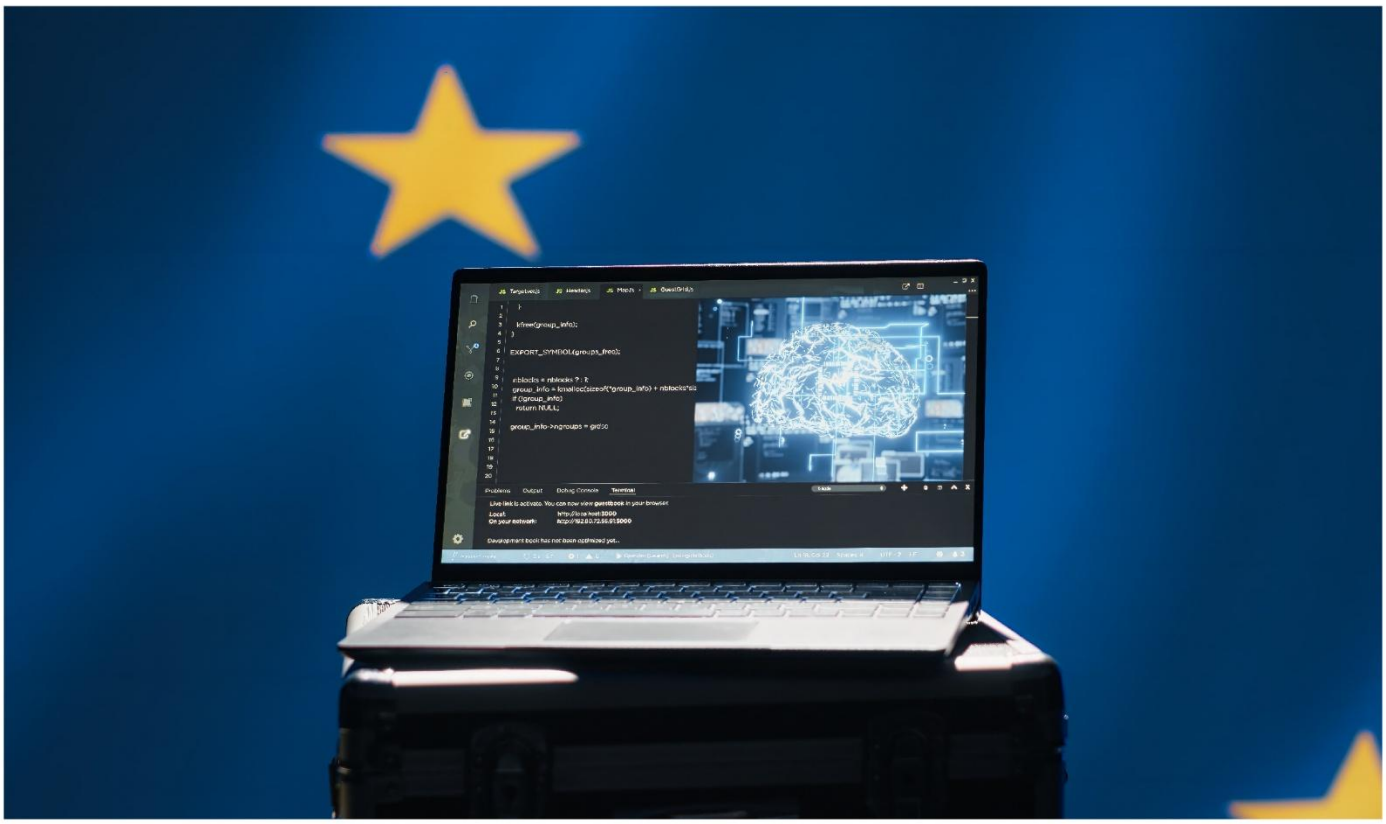
Emergency Resolution

Shielding Democracy and Enhancing Electoral Resilience



Approved by the EPP Political Assembly, 13 - 14 January 2025, Brussels

The EPP is the party of security, subsidiarity, and value-based politics and policies. Disinformation, misinformation, and Foreign Information Manipulation and Interference (FIMI) pose a growing threat to our democratic institutions and processes, such as elections, in Europe. All of the above constitute forms of hybrid threats and in their more extreme even forms of hybrid warfare. While these are not new phenomena, the wave of digitalisation, social media and Artificial Intelligence-enabled tools have fundamentally changed its reach and impact and increased cyber risks in a transformed security landscape. The growing influence of technology tycoons who misuse their power and operate social media platforms with insufficient oversight also raises significant concerns. Moreover, authoritarian states like Russia and its proxies have increasingly used FIMI with systemic and deliberate intent to undermine democracies and democratic electoral processes. They also have developed a highly organised state-sponsored system of interference and disinformation which constitutes an inherent part of their overall strategy of the "new generation warfare" with many different types of hybrid attacks and sabotage actions, which Russia waged on Europe and the West in general.

For example, we see that elections are increasingly targeted by anti-democratic forces to influence the outcomes in their favour, for example by preventing people from making informed choices or by dissuading them from voting. Recent examples of Russian interference in elections highlight efforts to exploit societal divisions, strengthen anti-European and far-right and far-left ideologies, destabilise governments and promote candidates aligned with Russia's strategic interests. Social media platforms and Artificial Intelligence-enabled tools have emerged as the primary battleground for these influence operations.

Our response must be firm: the European Union, as the largest promoter and supporter of democracy globally and itself one of the most successful democratic and peace projects in the world, must strengthen its resilience and make full use of all available means to prevent, deter and respond to foreign hybrid activities such as manipulation of information, interference and attempts at undermining democracy in electoral processes at all levels, including by propagating hate speech and hate crime in our societies. The impact of such activities is intensified by the lack of compliance with international standards for democratic elections, poor rule of law and centralisation of state powers. In addition, corruption and organised crime, provide pathways for malign actors to penetrate and influence elected officials and institutions.

There must be a clear strategic response to this strategic challenge. The "new generation warfare" waged by authoritarian states like Russia demands to respond with a strategy of "new generation defence". This defence strategy should be two-fold – strengthening European defence capabilities and weakening offensive warfare capabilities of authoritarian states, particularly Russia. We must mitigate Russia's hybrid threats and address Russia's attempts to influence political developments in the neighbouring countries.

We as the European People's Party stand united in tackling this continued threat, in calling for more and better-coordinated European action at all levels, in stepping up EU member states' defence and in taking party-political action. Hybrid attacks are real attacks on our security and deserve real actions.

1. We bring the fight of the European Union against misinformation and disinformation at a new level.

The defence of our democracy has been and will remain a key fight of the European People's Party. It touches all levels of governance of our Democracy. Europe needs a European Democracy Shield (EDS) now to counter foreign information manipulation and online interference with the implementation of key legislation and initiatives to boost the health of the information sphere. Therefore, for it to be successful, it should build on and integrate with the Digital Services Act (DSA), the EU Code of Practice on Disinformation, which should be made mandatory for Very Large Online Platforms (VLOPs) as per the DSA definition, the AI Act, the Democracy Action Plan and the wider Defence-of-Democracy Package. We cannot afford compartmentalisation when our democracy and information integrity may be at stake. As EPP, we want the EDS to be able to expand into the EU's neighbourhood to ensure a global approach in response to global strategies of authoritarian state actors. Supporting our neighbourhood is key as it helps counter tactics that often spread to the EU.

We shall also monitor more closely and actively defend against breaches of the Digital Services Act (DSA) and the EU Code of Practice on Disinformation. An increase of such EU-wide inquiries and investigations must ensure that social media platforms are held accountable. Autocratic led countries, including Russia and China, should not be allowed to exploit social media for fostering polarisation and undermining European democracies. We will take prompt action if companies running large platforms (such as X, Meta or TikTok) are found to be in breach of the regulations and have failed to act to mitigate risks relating to information manipulation, referral systems, advertising transparency and access to data.

The EU Hybrid Toolbox, the FIMI Toolbox and the Cyber Diplomacy Toolbox contribute to ensuring coordinated responses to hybrid campaigns, cyber-attacks and FIMI activities against the EU, but we want to use them in a more integrated manner. We will upgrade them based on lessons learnt from Ukraine's, Republic of Moldova's, Taiwan's and other countries' expertise in countering foreign interference and aggression.

Finally, we will take steps for the EU's early warning and monitoring systems to be reinforced through ENISA to track cyber threats and disinformation campaigns so EU member states can be alerted of risks in real-time, and for the European Cybersecurity Competence Centre and Network (ECCC) to be strengthened to increase the EU's cybersecurity capacities and competitiveness, in line with the Cybersecurity Act and the NIS2 Directive.

Overall, the EU must continue to fight FIMI and disinformation. The response to this challenge must focus on enforcing the rules both on gatekeepers as well as on the entire range of digital intermediary services, strengthening our democracies, our democratic electoral processes at the European, national, regional and local level, and protecting journalists and media pluralism, providing reliable information and raising awareness about disinformation and our preparedness and response, building societal resilience against disinformation through media literacy and fact checking, and cooperating with other institutions, national authorities and third parties. In particular, the big Tech companies and the companies running large platforms (such as X or TikTok) bear great responsibility in shielding democracy and enhancing electoral resilience, for example by programming algorithms in ways that they are not manipulatively spreading fake news and radicalisation. In the digital world we also believe in a social market economy model, but these social market economies have to be rules- and values-based. This starts with responsible enterprises for the common good.

2. As Europeans, we want to take the lead in building Defensive Democracy.

We acknowledge that FIMI is a national and cross-border security threat. Hence, the EPP is committed to strengthening democratic institutions and to building democratic resilience through cooperation. The EPP seeks to build even stronger domestic, regional, and global partnerships that are more assertive towards and resilient against the attempts of autocratic actors, who, working alone or through concerted action, undermine multilateral organisations, cause destabilisation and threaten global security. We urge our European heads of state and government to put the strength of our democracies into action to revitalise, to consolidate and to strengthen the international rules-based system that was constructed by leading democratic allies at the end of World War II. It is a system that is predicated on a set of norms and principles encouraging peaceful, predictable, and cooperative behaviour amongst states as well as formal institutional bodies, such as the United Nations (UN) and NATO that serve to legitimise and uphold these rules. These in turn provide an environment, in which democracies flourish. We welcome 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. The EPP believes that European democracies would do well to draw on the experiences and the expertise of countries in our Eastern Neighbourhood, particularly Ukraine, Moldova, Armenia and Georgia, which are subject to frequent disinformation campaigns launched by the Russian Federation and its proxies. Equally, the United States, Japan and Taiwan all have rich experiences in tackling disinformation. We, however, also call for closer cooperation on strategic communication to tackle the threats posed by malign foreign interference in countries of the Eastern Partnership and the Western Balkans. We are concerned about the developments in Romania after the recent elections. We underline the importance of combatting disinformation to contain anti-Western and divisive rhetoric which seeks to exploit and exacerbate ethnic tensions in countries that are particularly vulnerable.

We call upon our member states and the candidate countries to strengthen the security of our common and respective critical democratic infrastructures from repeated and even more sophisticated attacks, by ensuring each EU member state and each candidate country has a digital security architecture that defends our democratic systems against cyber-attacks. Our citizens are one of the greatest assets in our democracy. Strengthening the links and trust between people and the democratic institutions that represent them is the bedrock of democratic resilience. The EPP wants to empower citizens in both building a robust democracy and to resiliently defend when necessary. We can build further on key initiatives like the Conference on the Future of Europe and the European Citizens Panels. In this same vein, we recognise the need to support curricula to improve media literacy among citizens, to strengthen civic education and critical thinking by incorporating it in school systems at all grade levels, and to inform the public better also through national and regional parliaments and electoral authorities, to reduce or eliminate citizens' risk of information manipulation. Importantly, this should also be the case for lesser-spoken languages. For the same reason, we believe in more sustainable and long-term investment in our civil society organisations tackling information manipulation. Too often still, funding is project-based, relying on third country sources and not covering basic administrative costs or requiring unrealistic share of co-financing. We finally call for a recognised European network of fact-checkers available in all EU languages to all citizens.

3. The EPP wants to lead by example in taking party-political action.

Concerned about Russia's efforts to systematically create dependencies through European extreme right and left-wing, and populist political parties, we acknowledge the fact that electoral campaigning is shifting to the digital arena, which comes with great opportunities for engagement with audiences, but also with increased responsibility for a leading party like ours. As the EPP, we are strongly concerned that the disinformation campaigns and election interference carried out by Russia during recent European elections as well as in Romania, Moldova, and Georgia is just the beginning of a sustained attack on our European way of life. Where we bear political responsibility, we commit therefore to protecting the resilience and reliability of election infrastructure, including IT systems, voting equipment, election office networks and databases. We also commit to establish within the EPP family a communication and campaign expert network to pool and encourage data exchange on cases of foreign interference and election manipulation, which eventually may lead to the development of actions and practices that prevent and, where appropriate, react against this phenomenon. Our party and its members express their concerns over the influence on young users and the interference of TikTok. We stress the importance of the ongoing investigation of the European Commission and the measures to be taken to mitigate the serious concerns.

As the party of security and values-based politics and policies, we as the EPP are strongly determined to counter the attempts posed by authoritarian regimes and political forces that try to undermine European democracies. We strongly believe in strong democracies which are capable to defend themselves and their values by strong institutions and responsible actions.

Rue du Commerce 10
1000 Brussels
T +32-2-2854140
E connect@epp.eu

The publication of this document
received financial support from
the European Parliament.

If you have any question you would like to ask please contact us.