European Parliament
2024-2029

Special Committee on the European Democracy Shield

29.4.2025

WORKING DOCUMENT

on Protecting European democracy and our values

Findings and recommendations of the Special Committee on the European Democracy Shield

Special Committee on the European Democracy Shield

Rapporteur: Tomas Tobé

Introduction

In recent years, the European Union and its Member States have faced an escalating threat landscape, with foreign information manipulation and interference (FIMI), hybrid attacks, and disinformation campaigns orchestrated by malicious third-country actors among the emerging trends. These hostile activities aim to weaken the democratic foundations of the Union by sowing division, eroding trust in institutions, and exploiting societal vulnerabilities – often through increasingly sophisticated digital means. In this context, the need for a comprehensive, coherent, and future-oriented response has become more pressing than ever.

As a follow up to the work carried out by the special committees on foreign interference in all democratic processes in the European Union, including disinformation (INGE and INGE 2), and in response to the European Commission's commitment to creating a European Democracy Shield as one of the key actions for the current legislative term, in December 2024 the European Parliament decided to set up a Special Committee on the European Democracy Shield (EUDS).

This working document aims to contribute to mapping policy areas that, in the view of the EUDS Committee rapporteur, should be the focal points for relevant policy actions, while also making suggestions on what these actions could be. In addition, this document is meant to form the basis for discussions that will serve as an early contribution to the Commission's work on the planned Communication regarding the European Democracy Shield.

The working document underscores the importance of strengthening the Union's capacity to detect, deter, and counter FIMI and other hybrid threats. While acknowledging the important advances accomplished by the INGE and INGE 2 committees, as well as other related Parliament’s initiatives, the ever increasing intensity of interference and threats to our democracies show that much more progress needs to be made. This document highlights the need for the creation of a new independent structure, reinforcement of digital defense, and the promotion of the role of independent media and civil society. It also addresses the role of sanctions, the importance of democratic resilience beyond EU borders, and the necessity of fostering civil preparedness in an era of multidimensional crises.

1. EU structures to combat FIMI

The need to further strengthen Europe's collective capacity to detect, analyse and counter FIMI and disinformation campaigns from third countries is clear. It is also clear that different Member States have made varying kinds of progress in this work. Positive examples such as Viginum in France or the Swedish Psychological Defence Agency, can serve as role models for the work of other Member States.

Recent years have seen important development at the level of EU institutions. However, it is apparent that the EU is still suffering from a fragmented approach. Existing coordination mechanisms, such as the Rapid Alert System (RAS) should be reinforced. Overarching strategic goals are still lacking, which the Parliament has previously underlined by calling for a coordinated and comprehensive strategy against foreign interference. We cannot afford compartmentalization when Europe's democratic systems and institutions are under attack. We need to develop more effective tools and integrated approaches, and invest in expertise and capacity, at European and Member State level to tackle FIMI.

The rapporteur is of the opinion that this development requires the creation of a new independent structure at EU-level dedicated to combating FIMI. At the heart of such a future structure should be the ability to act rapidly and in a decisive manner against ongoing threats, based on situational awareness from Member States and EU institutions. There have been important investments in terms of detecting, analysing and understanding the FIMI threat but too little has been done to use this situational awareness to take robust and proactive action to address and neutralize the threat at the earliest possible stage, raising costs for the perpetrators, while also reinforcing long-term resilience building efforts in all Member States.

Such a new independent structure should build on existing work undertaken by the Commission, the European External Action Service (EEAS) and European Parliament through their strategic communication work, by the RAS and gradually become operational in its functionality. While acting as an information hub to guide and support Member States and EU institutions, it should function as a European centre for excellence for fighting FIMI. The interoperable methodology for FIMI detection and response, developed by the EEAS, and now also under development in the European Commission, could serve as a basis.

There is a need to take a holistic approach to how the European Commission as the executive EU institution, the EEAS and other relevant structures, handle FIMI related issues. Avoiding possible fragmentation and duplication of capabilities will be a key objective in this exercise. In this regard, it is important that a potential new structure is organised in such a way that it strengthens and connects capabilities of existing initiatives in the area of hybrid threats, cybersecurity and other relevant disciplines. Creating completely new structures is inherently complicated and new organizational models take time to get into place, and therefore a carefully calibrated approach making the best use of existing mechanisms in place is needed. The threat from foreign interference is urgent, ongoing and increasing.

The rapporteur further intends to examine the need for a regulatory framework to develop minimum standards for Member States' work on combating FIMI. A framework that can be designed in different ways (legislative and non-legislative tools, or a combination of them), but should aim to create an increased degree of common definitions, objectives, standardisation, interoperability as well as a single point of contact for FIMI-related work in each Member State.

The rapporteur notes the larger context in which the discussion on new organisational models for combating FIMI takes place. More specifically what the EU's role in more traditional intelligence work should look like in the future and how the EU's intelligence capabilities, such as the Intelligence and Situation Centre (EU INTCEN), should be developed and also serve the Union’s ability to counter FIMI and other hybrid threats. This should be considered as a separate, but linked, issue.

2. Digital resilience

FIMI, hybrid threats and disinformation campaigns pose a growing danger to democratic societies especially in the online space. These tactics – often blending cyberattacks, private messaging services, emails, and the use of social media – seek to undermine trust in institutions, polarize public opinion, and disrupt electoral processes. The digital space has become a fertile ground for malign actors to exploit vulnerabilities and shape how society thinks and behaves. Through social media algorithms amplifying content that generates high engagement, these actors exploit the very nature of human behaviour, where controversial or

negative content tends to drive more reactions, leading to its increased visibility. New technologies such as AI represent great opportunities for progress, but are also prone to be exploited, as recently reported with regard to a Moscow-based "Pravda" disinformation network deliberately infiltrating large language models with pro-Kremlin deceptive narratives.[1]

In recent years, the EU has recognized this evolving landscape and responded with a stronger regulatory framework designed to protect its information space. Among others, the Digital Services Act (DSA) and the Regulation on the Transparency and Targeting of Political Advertising are two key pillars in this defence. The DSA introduces binding obligations for online platforms to take down illegal content and detect and mitigate systemic risks, including the spread of disinformation and the misuse of automated accounts. Meanwhile, the Political Advertising Regulation aims to increase transparency around who is behind political messages and how they are targeted. Together, these laws represent an important step forward in holding digital platforms accountable and protecting democratic processes. Additional elements of newly adopted rules, such as the requirement in the AI Act for labelling AI generated content such as deepfakes, intend to complement EU's protection of the online space. The rapporteur's aim will be to observe timely and correct implementation of the EU's digital acquis, with a particular focus on the DSA, and examine the challenges linked to non-compliance.

Freedom of expression and information is a key fundamental right to be upheld in this endeavour, applicable to the offline and online space alike. The EU benefits from one of the strongest protections of human rights worldwide and companies wishing to operate in our space and attract European customers have a shared responsibility to safeguard these rights. This applies particularly to online platforms which have developed a unique role in the information space and citizens are expecting this space to be trustworthy and democratic. The DSA should continue to uphold this very right of free speech, with appeal mechanisms for content takedowns for users on one hand, and faithful risk assessment and mitigation measures by the companies on the other.

The rapporteur further intends to look at individual phenomena that are increasingly posing danger in our online space. Recent events like the presidential elections in Romania demonstrate how the use of fake accounts, bots, and selective amplification of particular political content or candidates may be exploited by foreign malicious actors to influence the outcome of a vote. TikTok's claims of deleting 116,000 spam accounts and 59,000 fake accounts as a follow-up testifies the gravity of this problem.[2] In addition, political opinions are being shaped by online influencers operating on the edge between product advertising and journalism, often without requirements for transparency, accountability, and informational quality. Driven from the examples from the Romanian elections, it should particularly be looked at how foreign interference actors are instrumentalising many nano- and micro-influencers to spread disinformation, as they may be more willing to cooperate than individuals with a larger follower base, through fake marketing companies hiding their identity. Further assessment of these phenomena will be required to determine whether existing EU legislation, if correctly implemented, covers them in scope, or whether there are remaining legal gaps to be filled. New initiatives as part of the announced Digital Fairness

[1] https://www.newsguardtech.com/special-reports/moscow-based-global-news-network-infected-western-artificial-intelligence-russian-propaganda/

[2] https://newsroom.tiktok.com/en-eu/continuing-to-protect-the-integrity-of-tiktok-during-romanian-elections

Act or the Digital Package will be of key interest in this regard. The rapporteur will also research best practices to fight AI-manipulated content, including disinformation red teaming and crisis preparation in organisations and political institutions, building and leveraging public-private partnerships, establishing AI safety and security strategies and more.

The rapporteur's assessment will also look at individual stakeholders and their compliance with the adopted rules, noting with concerns that several large tech companies are currently under the Commission's investigation for potential violations of the DSA. In light of the above, formal proceedings have been opened against TikTok on election risks under the DSA[3], and their swift finalisation will be key in order to contain the possible damage but also maintain trust of citizens in the legal framework and the institutions. Worrying questions are also arising around Telegram and its possible role in facilitating criminal activities and foreign interference in the EU. Further investigation into the originally Russia-founded platform as well as accurate calculation of its monthly active users and its possible classification as a very large online platform (VLOP) under the DSA needs to be finalised as soon as possible. To increase citizens' protection and ensure a level playing field of the platforms, Telegram is also strongly encouraged to sign up to the Voluntary Code of Practice on Disinformation.

Finally, the European Commission and EU Member States should prioritize fostering homegrown innovation and technological development as a strategic counterbalance to the growing influence of foreign tech giants within the EU, notably hailing from the U.S. and China. By investing in digital infrastructure, supporting startups through funding and regulatory sandboxes, and strengthening public-private partnerships, the EU should cultivate a more competitive and sovereign digital ecosystem. Encouraging innovation and deployment in areas with critical dependencies such as data centres, cloud and edge services will not only reduce reliance on non-European platforms but also enhance resilience, data autonomy and sovereignty. This approach should involve building secure local data centres, and European sovereign cloud infrastructure can be developed through market solutions. Moreover, aligning innovation policies with ethical and democratic values can position the EU as a global leader in responsible tech, setting standards that reflect its commitment to transparency, human rights, and digital sovereignty. This may eventually lead to a natural development of a European social media platform that would embed such principles in its very design.

3. Media, information integrity and fact-checking

Media is an irreplaceable part of our democracies and independent journalism is in many ways the antidote to disinformation. Policies aimed at upholding and promoting free and independent media should therefore be an important part of the European Democracy Shield. The EU must work to ensure basic protection for the media sector through new initiatives, rule of law monitoring and full implementation of the European Media Freedom Act (EMFA). At the same time, we need policies that make media financing models work long term. Policies and legislation concerning, for example, consumer protection, advertising or digital platforms, needs to be designed with a particular attention to how the regulations will affect news media, both public and private.

The rapporteur emphasizes the importance of active work on improving media literacy and welcomes the Commission's ambitions to strengthen the EU's efforts in this regard. The work

[3] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487

already being carried out in the form of guidelines from the Commission, and the minimum requirements set out in the Audiovisual Media Services Directive (AVMSD), need to be evaluated and further reinforced. Funding opportunities and assessment of the effectiveness of media literacy projects, currently part of frameworks such as Creative Europe, should also be analysed.

In the effort to promote independent media, the EU should take measures to strengthen journalism education within the Union. Both in terms of students and professional journalists, more could be done to increase the exchange within the EU. It should for example be explored how the Erasmus+ program could play a greater role in this effort.

Threats, violence, sabotage or other forms of actions aimed at hindering the work of journalists constitute a widespread problem that in itself puts democracy under pressure, and which can serve as a tool for hostile third-country actors to undermine our democracy. Last year, the Media Freedom Rapid Response documented 1,548 press freedom violations targeting 2,567 media-related persons or entities in 35 European countries – an alarming increase compared to the 1,153 violations recorded in 2023[4]. The rapporteur recognises the important steps already taken at EU level to increase the protection of journalists, not least through the EMFA and the Anti-SLAPP Directive. Effective and careful implementation of these instruments must be observed with utmost importance. The nearly five-year-old recommendation from the European Commission regarding the protection and safety of journalists needs to be evaluated and possibly updated to take into account the development of new emerging threats.

Covert actions of foreign powers within the media market in Europe pose a serious threat that should be addressed within the framework of the European Democracy Shield. The European Parliament has previously expressed concern about the possibility of media company takeovers by foreign entities under the direct or indirect control of malicious third-country actors. There are numerous examples of this, particularly Russian actions in the media landscape in Eastern and Central Europe. But we have also seen other examples, such as how the Iranian regime has acted on the Spanish-speaking media market. The revision of the foreign direct investment screening framework, proposed in 2024, has the potential to be an important tool in this regard, as well as the provisions concerning non-EU providers targeting EU audiences in the EMFA. The rapporteur intends to further explore the need for additional Union measures.

The US administration's decision to change its aid policy has had an impact on the media market both within the EU and in the EU's immediate vicinity. It is important that the EU and its Member States analyse these consequences and, if necessary, act to fill the void left. A notable example is the case of Radio Free Europe, whose survival is of strategic interest to the Union, in addition to many other examples, which shows the need to find a solution to secure structured funding for these important projects aimed at protecting democracy. The question of long-term economic viability, especially in the case of independent and local media, is a larger issue that needs further attention.

To combat disinformation and provide valuable insights for DSA risk assessments civil society-based networks of fact checking can play a crucial role. Ensuring that actors who contribute to fact-checking have long-term conditions under which to operate is, in this

[4] https://www.ecpmf.eu/mfrr-monitoring-report-2024/

respect, a step toward upholding Union legislation. Existing projects, such as the European Digital Media Observatory (EDMO), represent an important way for the EU to support fact-checking organizations. The announced European Network of Fact-Checkers should incorporate the existing European Fact-Checking Standards Network (EFCSN).

4. Civil society

Civil society plays a key role both in exposing and combating foreign attempts to interfere with democratic processes, and in the long-term effort to build societies that are more resilient to such attempts. It is also important to emphasize that civil society's role in monitoring and upholding the values enshrined in Article 2 TEU. As clearly illustrated by the ongoing Russian war of aggression against Ukraine, civil society is a crucial actor when communities are in crisis situations. These insights should be reflected in the work of the European Democracy Shield.

The rapporteur welcomes the Commission's ambition to present a European Civil Society Strategy in 2025 and is of the opinion that the work on this strategy should be integrated within the framework of the European Democracy Shield.

It is of great importance that legislators, both at the national and EU level, design legislation that takes civil society into account and empowers it. Correspondingly, the financial conditions for civil society are crucial, which is why sustainable and long-term investment in our civil society organizations should be a priority. This should be done both through public commitments and through various measures that promote philanthropy.

The ability of civil society to operate is also deeply intertwined with rule of law conditions within the Union, which underscores the importance of ensuring that the European Democracy Shield is coordinated with the work on the Rule of Law Dialogue and the Annual Report. The rapporteur intends, for this purpose, to further explore the possible need for new ways to strengthen the protection of civic space.

While we strive to protect civil society and promote its role in society and decision-making processes, we must simultaneously note that civil society organizations can, and have been, used as tools by third-country malicious actors to illegitimately influence democratic processes in the EU and its Member States. The rapporteur welcomes the Commission’s ambition to increase transparency regarding third countries’ use of CSOs, through the proposal for harmonized requirements on transparency of interest representation, and calls on the co-legislators to move forward with the process. Further measures to increase transparency and make it more difficult for malicious actors to operate covertly within democratic systems using CSOs should also be considered. At the same time, these measures should be designed in a way that prevents them from being misused to stigmatise the legitimate activities of civil society as such.

5. Cybersecurity and protection of critical infrastructure

The Democracy Shield also needs to look at the protection of critical infrastructure and entities. Hybrid attacks targeting critical infrastructure in the European Union have become a growing concern, with incidents linked to the same malicious actors such as Russia, China, but also Iran. These attacks often target essential systems, networks, and facilities that are vital for a society's functioning, including public safety, security, and economic stability. For instance, the Baltic Sea has witnessed multiple disruptions to submarine cables, which are

vital for internet connectivity and power supply. Since 2023, at least 11 such cables have been damaged, painting a picture of coordinated sabotage.[5] Arson attacks targeting critical infrastructure in various EU Member States, such as the recent case of incendiary devices used at Leipzig airport, further confirm the complexity of hybrid warfare performed against the EU. In addition, Europe is facing a surge in cyberattacks, including breaches of government systems, data theft, and espionage. All these incidents underscore the need for enhanced security measures and international cooperation to safeguard Europe's physical and digital integrity. These efforts should strengthen links between law enforcement, security and cybersecurity services, military and civil protection, as well as private operators.

Of major concern remains EU's dependence on foreign actors and foreign-made technologies in critical infrastructures and supply chains – not the least with regards to critical raw materials, semiconductors and medicines – and the vulnerabilities created by foreign direct investment (FDI) being used as a geopolitical tool. Our reliance on external suppliers and technologies represents one of its most significant vulnerabilities. The recently launched European Internal Security Strategy (ProtectEU Strategy) explicitly acknowledges that "our dependencies on third countries in terms of supply chains make us more vulnerable to hybrid campaigns by hostile states".[6] Attacks on supply chains through software dependencies, in particular, have emerged as the top cybersecurity threat projected for 2030, according to the European Union Agency for Cybersecurity (ENISA).[7]

While there have been a lot of advancements in the legal framework focused on the protection of critical infrastructures and cybersecurity, further research and work needs to be devoted to ensure its completeness. The rapporteur welcomes that the Parliament's calls on the Commission to develop "ambitious binding ICT supply chain security legislation" and a "stronger regulatory framework to the FDI Screening Regulation" were met by the adoption of the Cyber Resilience Act and the presentation of the proposal for revising the Foreign Direct Investment (FDI) screening regulation.[8] The latter is yet to be finalised by the co-legislators. One of the main stumbling blocks in the efficient implementation of the EU legal framework remains the low level of transposition of the NIS2 Directive. Following the October 2024 deadline, the Commission had to send letters of formal notice to as many as 23 Member States for failing to fully transpose the Directive.[9] The rapporteur in this regard welcomes the Commission's pledge to work closely with Member States to ensure a swift and coherent implementation of the horizontal cybersecurity framework set out in the NIS2 Directive, as well as the Cyber Resilience Act and the Cyber Solidarity Act, as stipulated in the ProtectEU Strategy. The revision of the 2019 Cybersecurity Act along with the reassessment of the mandate of ENISA, the upcoming EU Ports Strategy or the revision of the EU procurement rules will all be initiatives where Europe's security needs to stay at the centre. Appropriate funding for cybersecurity measures in EU institutions, bodies, offices and agencies should also be observed. The rapporteur will also aim to further investigate Europe's vulnerabilities with regard to the uptake of new technologies including AI, 5G and 6G

[5] https://www.politico.eu/article/russia-sabotage-undersea-cables-baltic-sea-europe-war/

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025PC0148

[7] https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Foresight%20Cybersecurity%20Threats%20for%202030.pdf

[8] INGE 2 Report, paragraph 62

[9] https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive

networks, cloud services and quantum computing.

6. Justice and Home Affairs

In addition to specific proposals and tools that will be established within the framework of the European Democracy Shield, as well as existing ones that clearly fall within the scope of the Shield, a valuable contribution may also originate from Union instruments which objectives only partially align with those of the European Democracy Shield. The rapporteur intends, in this regard, to explore the capabilities available within Union agencies and related networks for national authorities' cooperation in the area of justice and home affairs (JHA), in an effort to examine ways to fully exploit the potential of instruments aimed at upholding the democratic values of the Union.

In its latest Serious and Organised Crime Threat Assessment, the European Union Agency for Law Enforcement Cooperation (Europol) has warned about the double destabilising effect that serious and organised crime has on the EU and its Member States in that it is progressively becoming a vehicle for hybrid attacks.[10] However, Europol's mandate currently does not cover sabotage, hybrid threats or information manipulation. In his work, the rapporteur intends to make an early contribution regarding how the planned revision of Europol's mandate can be used to meaningfully strengthen the objectives set out by the European Democracy Shield.

The same can be said regarding the European Union Agency for Criminal Justice Cooperation (Eurojust), which also has tasks that overlap with the fight against hybrid influence, and whose mandate, according to the newly launched ProtectEU Strategy, is set to be revised. The example of the DSA shows that the current legislation on hybrid threats and disinformation focuses a lot on the component of law enforcement, but not as much on the judicial one, even though both are part of the security chain. As part of the revision, the European Commission should therefore identify legal gaps where Eurojust has a potential to address these threats more efficiently, but currently is not allowed to do so. Furthermore, Eurojust faces a number of challenges that should be addressed in the context of other related policies, including the lack of a harmonised legal framework for data retention or differences in the definition of migrant smuggling in the various Member States.

Union agencies with responsibilities in the area of borders, migration and asylum management. i.e. the European Border and Coast Guard Agency (Frontex) and the European Union Agency for Asylum (EUAA), have another key role to play, in cooperation with national authorities, in establishing and maintaining common situational awareness on risks related to the exploitation of migratory flows for political purposes and in assisting frontline Member States in situation of crisis. It would thus be relevant to discuss ways to strengthen their capabilities in those areas in the context of the European Democracy Shield.

The role of Frontex, in particular, could be enhanced as regards hybrid threats and instrumentalisation of migration as well as in the field of security. In the context of revising its founding regulation, the Agency could be mandated to operate in high-risk security environments, provide support for the protection of critical infrastructures and strengthen border crisis management, as well as engage in enhanced information collection and information sharing with relevant national, EU and international authorities.

[10] https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime

7. External Action

Promoting democracy and the rule of law globally is an obligation embedded in the EU Treaties, and it is important to maintain a clear connection between defending democracy within the Union and supporting it abroad. In the fight against FIMI, supporting efforts in countries located close to the EU – particularly candidate countries – should be a priority. In many ways, these countries are significantly more exposed to FIMI operations than EU Member States themselves. They often serve as testing grounds, due to also their limited capacities, for strategies utilised later against Member States. In addition the EU will also need to take more robust measures against adversaries' globally expanding FIMI operations which seek to undermine the EU's standing also in Global South and beyond.

When it comes to candidate countries, the EU should support them to counter continuous use of FIMI and other hybrid activities to attempt to derail them from their European path. We must also recognise that today's candidate countries will eventually become Member States, meaning that what are now external challenges will, in the future, become internal ones. This conclusion holds true across many policy areas, but is especially relevant when it comes to safeguarding democracy.

Against this background, the European Democracy Shield should also have an external dimension. The efforts of the European Commission, the European Parliament and EEAS to build resilience against FIMI, strengthening democratic processes and ensuring electoral integrity in partner countries in the Eastern and Southern neighbourhoods, the Western Balkans and Sub-Saharan Africa, is of great importance. These efforts – and the flagship project, EUvsDisinfo – should be further strengthened, going beyond just targeting pro-Kremlin actors and addressing the serious hybrid threats posed by countries like China, Iran and other state and non-state actors.

The rapporteur also intends to explore and make recommendations on how the EU's external presence, including EU Delegations and CSDP missions, can more effectively serve as a first line of defence against cyber and hybrid attacks and countering FIMI threats and strengthen CSDP missions' resilience in the countries of their deployment

International cooperation with like-minded partners, particularly within the frameworks of the G7 and NATO, but also multilateral cooperation within international organizations such as UN, CoE, OECD as well as the ongoing development of Security and Defence Partnerships, should be an integral part of the external dimension of the European Democracy Shield, with the aim for more robust responses against the FIMI threat.

8. Election systems and electoral resilience

A core objective of the European Democracy Shield is to protect the integrity of elections, at local, regional, national and European level. Free and fair elections, without interference, are fundamental to democracy. Even though Member States have different democratic traditions and conduct their elections in various ways, there are still good reasons to continue cooperating at the European level in exchanging best practices and formulating common norms, as illustrated by the Commission's recommendations regarding resilient electoral processes in the Union. Work of the Member States and EU institutions should continue, to inform citizens of their rights and electoral processes, to empower citizens to participate in voting and to make them more resilient against disinformation campaigns targeting the elections.

An important tool for exchanging experiences between Member States and EU institutions regarding electoral resilience is the European Cooperation Network on Elections (ECNE). This network serves as a crucial foundation for joint expertise by enhancing sharing of best practices related to the integrity of elections, as well as building a strong network of European electoral experts. The rapporteur intends to explore the possibility of further enhancing the role of ECNE by examining how the network can play a greater role in future efforts to strengthen European electoral systems.

As the digitalization of our societies increases, more and more electoral processes are incorporating digital elements. Not necessarily through digital voting, although such examples also exist in some Member States, but rather the processing of information related to electoral processes by digital means. This creates a potential vulnerability that Europe needs to become better at managing, to ensure the highest level of data protection and cybersecurity. To this end, the Rapporteur will suggest that digital election infrastructures be added as an essential service of public administration in the annex of the Critical Entities Resilience Directive.

The physical security of candidates in elections is a central part of democracy. Hate campaigns and violence that discourage and make it difficult for candidates to participate in the public debate or interact with voters constitute a threat to democracy. Such threats can also be fuelled by third countries' attempts to destabilise Europe. Candidates belonging to minority groups, as well as female politicians, are particularly targeted. The Rapporteur intends to look into relevant EU measures that can support Member States' efforts to ensure the physical protection of candidates.

The actions of foreign actors within the party political landscape in Europe, especially various cases of funding extremist movements by third countries, play a role in the broader discussion about foreign influence on European democracy. The most important measure to address this is further requirements for financial transparency and auditing. The rapporteur would also like to explore further strengthening of operational information exchange in relation to financial forms of interference in elections, particularly between financial intelligence units, law enforcement and other competent authorities. The rapporteur further notes, in this context, the efforts of the co-legislators to find a common position regarding the revision of the regulation of the statute and funding of European political parties and European political foundations.

9. The role of sanctions in the protection of democracy

Attribution, cost increase, revenue cuts and denial of access through restrictive measures are key elements in our fight against the perpetrators of foreign interference in the EU. In this regard, the EU needs to move away from a defensive posture towards an offensive strategy. Particularly against Russia, by February 2025 the Union imposed a total of 16 packages of massive and unprecedented sanctions in response to its military aggression against Ukraine.[11] Sanctions have been imposed also in relation to a broad range of Russia’s hybrid activities, including cyber-attacks, information manipulation and interference campaigns, cases of arson, vandalism and sabotage and weaponisation of migration. On 8 October 2024, the Council additionally established a new framework for restrictive measures in response to Russia’s destabilising actions abroad.[12] And for its complicity in Russia's military aggression against

[11] https://finance.ec.europa.eu/news/eu-adopts-16th-package-sanctions-against-russia-2025-02-24_en

[12] https://www.consilium.europa.eu/en/press/press-releases/2024/10/08/russia-eu-sets-up-new-framework-for-restrictive-measures-against-those-responsible-for-destabilising-activities-against-the-eu-and-its-member-states/

Ukraine and other repressions and abuses, the EU has also targeted Belarus.[13] The rapporteur emphasizes that the assessment of imposed sanctions with regard to their best efficiency and possible further expansion should be an ongoing exercise. This should also include the consideration of secondary sanctions targeting those who engage in trading with the sanctioned entity, providing them with financial assistance, or engaging in other activities that are prohibited by the restrictive measures.

A new EU legislation on harmonising rules for criminalising the violation of EU sanctions was adopted in April 2024 in order to ensure adequate enforcement of the various sanction regimes in place. In this regard, the rapporteur reminds the Parliament's calls for assessing the competences of the European Public Prosecutor's Office in order to include investigation and prosecution of sanction violations throughout the Union.

As also highlighted by the INGE 2 report, moving away 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 built on objective criteria should be given careful consideration. Identifying and naming source countries, rather than individuals or companies, would be an important step towards acknowledging the problem of clear systematic and multi-layered interference that countries like Russia or China are performing in Europe. The EU currently maintains a list of high-risk third countries under the Anti-Money Laundering Directive (AMLD), which identifies jurisdictions that pose a danger to the EU's financial system and the proper functioning of the internal market. Particularly with growing evidence of Russia's involvement in money laundering and terrorist financing, the Commission should urgently finalise its assessment of listing the country as high-risk. In addition, the EU should make full use of its recently adopted Anti-Money Laundering Regulation which will provide additional legal bases for identifying dangerous countries, including those involved in the proliferation of weapons of mass destruction.

Beyond the framework of anti-money laundering and countering the financing of terrorism, further research should be devoted to the intersection of foreign interference and the area of criminal law. It is evident that all Member States are directly or indirectly targeted by the same third country malicious actors whose goal is to destabilise the Union as a whole, and therefore further joint solutions should be investigated. Article 83(1) of the TFEU allows to establish minimum rules concerning the definitions of criminal offences and sanctions with a cross-border dimension or where such crimes need to be combatted on a common basis.

10. European Union's preparedness

EU and worldwide developments show that hybrid threats and attacks may lead to full-scale and cross-sectoral crises with detrimental effects on safety and security, the well-being of citizens and the functioning of society and economy as a whole, constituting a key challenge to our internal affairs. This new reality needs to be reflected by the Democracy Shield as well. It will require a more robust approach to Union crisis management and civilian and defence preparedness, building strategic foresight and anticipation and strengthening early warning, detection, analysis and operational coordination capabilities.

Achieving a high level of civilian and defence preparedness will require a comprehensive, whole-of-society, whole-of-government, and all-hazards approach that integrates Member

[13] https://www.consilium.europa.eu/en/policies/sanctions-against-belarus/

States' authorities together with EU institutions, bodies and agencies, as well as businesses, academia, civil society and individual citizens. A robust common risk assessment framework will need to be established to identify vulnerabilities across sectors, from cyber threats and energy disruptions to military conflicts and natural disasters. This should be complemented by enhanced information exchange and clear coordination mechanisms between civilian and military actors, ensuring that emergency response efforts are swift, efficient, and well-resourced. At the same time, a clear and realistic communication strategy, as streamlined as possible, within the EU will be needed.

Additionally, preparedness must be embedded into everyday policymaking, with resilience principles guiding infrastructure development, supply chain security, and technological innovation. Investments in dual-use capabilities – such as logistics, communications, and medical resources – can enhance both civilian and military readiness. Public engagement is equally essential; raising awareness and equipping citizens with the knowledge and resources to sustain themselves during crises (such as the ability to manage for at least 72 hours without external assistance), to know where to seek shelter or how to help vulnerable and elderly people, can significantly improve overall resilience.

In his report, the rapporteur will aim to explore relevant areas of the concept of preparedness, building upon the report by Sauli Niinistö titled "Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness" as well as the EU Preparedness Union Strategy. In the above context, future research may be conducted on readiness, foresight and anticipation as well as population preparedness, on how to strengthen resilience of vital societal functions, crisis response and energy security, or how to make better use of civil-military cooperation, public-private cooperation and create resilience through external partnership. The rapporteur will also particularly consider practical ideas such as the creation of an EU-wide alert app, a household preparedness booklet, or a civilian crisis preparedness training or educational programmes. A comprehensive approach to training should be applied, involving all relevant stakeholders in the entire value chain including police officers, firefighters, as well as judges, clerks and regulatory authorities, and ultimately all interested citizens, with the aim to defend against foreign interference and manipulation and prepare for crisis scenarios. As part of a European solution, further expansion of the Erasmus+ programme should be explored.

By fostering a comprehensive and cross-sectoral and a whole-of-society culture of preparedness, supported by regular training exercises, scenario planning and emergency protocols, and with the allocation of appropriate funding, Europe can ensure it is ready to face a broad spectrum of emerging threats. In the heart of the European Union's preparedness lies the mutual assistance clause under Article 42(7) TEU, a mechanism to provide aid and assistance by Member States to another Member State that is the victim of armed aggression on its territory. For these cases, we must ensure that every actor, whether public or private, is aware of his or her tasks and duties. To protect ourselves, the European answer needs to be bold, clear and without a doubt that: **an attack on one of us is an attack on all of us**.