

FORGING THE EUROPEAN DEMOCRACY SHIELD

Policy Brief No. 159, May 2025

Europe has been thrust in the eye of the global geopolitical storm. The European Union faces pressure from the US to shoulder bigger democratic leadership, defence and geoeconomic responsibilities, while fending off Russia's assault on Ukraine and European democracy, and escalating hybrid threats and economic weaponization targeting internal governance vulnerabilities. In response to this evolving environment, the EU has embarked on a progressive strengthening of its security and defence posture. This evolution signifies a move beyond its traditional focus on external crisis management towards a more comprehensive and integrated approach to European security and preparedness. This approach prioritizes building resilience across critical sectors, pursuing greater strategic autonomy in key areas, fostering deeper cooperation among Member States and with international partners, and of course, countering hybrid warfare.

The EU, though under geopolitical pressures, has developed its democratic resilience, economic security, defence and internal security and rule of law capabilities to counter hybrid war tactics. It now needs to bind them all together and empower its institutions for both - enforcing relevant safeguards internally, and projecting geopolitical power externally - through increasing funding and building a network of coalitions of the willing within the EU. The **European Democracy Shield** initiative of the European Commission¹ should be the binding instrument, providing additional funding and cohesion for the EU's institutional response, consolidating rule of law capabilities, enforcing digital and democratic resilience initiatives, complementing the robust cybersecurity and infrastructure resilience outlined in European Internal Security Strategy ProtectEU,² and broadly protecting European democracy.

¹ European Commission, *European Democracy Shield*. See also: Ursula von der Leyen, *Europe's Choice. Political Guidelines for the next European Commission 2024 – 2029*, Strasbourg, 18 July 2024.

² European Commission, *ProtectEU: a European Internal Security Strategy*, COM(2025) 148 final, Strasbourg, 1 April 2025.

KEY POINTS

- The EU should systematically identify and address **vulnerabilities exploited by external actors through state capture methods**. Governance diagnostics tools, such as CSD's State Capture Assessment Diagnostics (SCAD), can effectively target reform efforts in critical sectors including energy, judiciary, and media.
- Economic coercion by authoritarian states can be countered by **linking economic security to democratic stability** through diversification of energy sources and supply chains. Reforms should eliminate vulnerabilities in strategic sectors and strengthen sanctions against complicity.
- **Media capture** should be countered through increased transparency in media ownership, targeted financial support for independent journalism, and strengthened regulatory frameworks to protect media pluralism and integrity across the EU.
- **Next-generation societal resilience measures** should include evidence-based interventions that promote algorithmic awareness and psychological resilience to manipulation, as well as ongoing civic education initiatives, independently managed at the EU level to ensure autonomy from state capture influences.

While the primary responsibility for directly countering Foreign Information Manipulation and Interference (FIMI) rests with dedicated structures like the EEAS East Strat-Com Task Force and specific regulatory instruments such as the Digital Services Act,³ ProtectEU makes a comple

³ *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)*.

mentary contribution to this effort by strengthening the overall resilience of the Union, particularly within the digital domain. Its emphasis on enhancing cybersecurity across the board serves as a crucial underpinning for FIMI defence. By proposing a new Cybersecurity Act and measures to secure cloud and telecommunications infrastructure, it aims to make the digital environment less permeable to hostile actions, in synergy with the dedicated EU FIMI Toolbox.

The EDS provides a key opportunity for building upon EU's recently developed and implemented instruments to tackle foreign interference into one comprehensive toolkit, supercharging its core focus on democratic resilience with links to governance, economic security and defence preparedness. It will complement the robust cybersecurity and infrastructure resilience outlined in ProtectEU. The Center for the Study of Democracy (CSD) has provided an actionable blueprint in its Kremlin Playbook series, which would add teeth to the Democracy Shield - real-time capabilities and defence-economic tie-ins, needed to respond to the multi-front, high-speed assault the EU is facing.

Target the State Capture Model

CSD's state capture framework exposes how external actors exploit governance weaknesses to infiltrate and manipulate state institutions, economies, and decision-making processes. It's about systemic corrosion, such as energy dependencies, corrupt elites, or captured regulators, and how external actors use economic leverage, political patronage, and institutional gaps to erode democratic resilience. This framework offers a practical lens to shift to a proactive, governance-rooted strategy, building upon the existing Rule of Law mechanism. The European Commission should integrate:

- **A monitoring and enforcement muscle** built into the Rule of Law cycle. CSD emphasizes identifying "capture points" (power concentration hubs) - sectors or institutions (e.g., energy, judiciary, media) where external influence thrives due to weak governance. The EDS could adapt best practice instruments such as the *State Capture Assessment Diagnostics* (SCAD)⁴ and *Monitoring Anti-corruption Policy Implementation* (MACPI)⁵ tools to assess Member States' vulnerability to state capture, prioritizing rapid reforms in high-risk areas. This would mean fast-tracking EU-level action (e.g. through the European Public Prosecutor's Office

– EPPO) and funding for institutional fixes (e.g. through Structural Reform Support facility). This would create a governance sprint or elevator for reforms - short, targeted reform cycles (e.g. 6-12 months) to plug capture gaps.

- **Act regionally and locally** through customization: Influence tactics vary by region and target specific governance vulnerabilities. In countering these influence tactics, the EU should adopt a tiered approach: tailored governance fixes for groups of Member States with similar vulnerabilities and/or willingness to act. Context specific reforms would make the democracy shield initiative more agile and would remove the sheer scale asymmetry – no EU country is a match for China's size and capabilities, and Russia's malign intent.
- **Countering state capture through sanctions enforcement:** CSD's "unvirtuous circle" model⁶ shows how economic ties (e.g., Russian strategic investment and corruption) translate into political sway. A focus on elite accountability: asset declarations, cross-border financial tracking, and sanctions for complicit actors should be reinforced. The focus should be on countering the illicit financing of Russian influence operations. The Anti-Money Laundering Authority (AMLA) and the European Public Prosecutor's Office (EPPO) must be equipped with enhanced mandates, resources, and cross-border cooperation tools to investigate and prosecute these crimes.
- **Energy and economic resilience as democratic pillars:** CSD links state capture to economic coercion. Russia has weaponized energy dependence,⁷ cutting gas flows and pushing narratives to fracture EU unity. China's economic coercion, like rare-earth export curbs and export embargos threaten Member States. This overarching umbrella needs to tie economic resilience to democratic stability, e.g. by countering disinformation that exploits economic pain through linking energy diversification and supply-chain autonomy to its mission. Economic resilience should be integrated into the governance playbook—fast-tracking diversification or antitrust measures against foreign monopolies. This would help cut the financial lifelines that fund influence ops, making democratic institutions less corruptible.
- **Positive economic statecraft:** The EU's many existing instruments should be leveraged for crowding out investment in areas prone to strategic corruption threats. InvestEU and STEP could fund tech innova-

⁴ Stoyanov, A., Gerganov, A. and Yalamov, T., *State Capture Assessment Diagnostics*, Sofia: Center for the Study of Democracy, 2019.

⁵ Stoyanov, A. et al., *Monitoring Anti-Corruption in Europe: Bridging Policy Evaluation and Corruption Measurement*, Sofia: Center for the Study of Democracy, 2015.

⁶ Shentov, O., Stefanov, R. and Vladimirov, M. (eds.), *The Kremlin Playbook in Europe*, Sofia: Center for the Study of Democracy, 2020.

⁷ Vladimirov, M., Levi, I. and Raghunandan, V., *Sanctions hypocrisy. G7+ imports EUR 1.8 bn of Turkish oil products made from Russian crude*, Sofia: Center for the Study of Democracy, 2024.

tions that bolster democratic resilience, prioritizing media pluralism, electoral integrity, and rule-of-law-compliant digital infrastructure. A new Digital Europe Programme funding window could support AI tools for detecting media capture and disinformation, alongside localized digital solutions to counter platform monopolies. Cohesion funds could target high-risk regions with investments in independent media, civic tech, and hybrid threat analytics, guided by European values and shielded from political meddling.

Better integrating the democracy shield initiative into the wider EU defence toolbox by adding a governance angle drawing on CSD's state capture framework could significantly enhance Europe's relevance and effectiveness in today's geopolitical climate, especially given the EU's need for rapid, actionable reforms to counter hybrid threats from Russia and others. This framework would reinforce the impact of the core focus areas of the European Democracy Shield of democratic resilience to hybrid threats, civic and media action.

Integrated Rapid Response to Hybrid Threats

Russia's real-time disinformation campaigns tied to Ukraine (e.g., amplifying energy crisis fears or sowing division over sanctions) and China's cyber ops demand a faster, more agile counter. Europe needs to close quickly the notable disparities in EU Member States' responses to FIMI. The EU has created considerable capacity at central level, yet it is still no match for the military-grade threats from Russia and China, and very often the most affected countries lack the capacity or political will to combat information interference threats, while others actively amplify disinformation.

- **A dedicated rapid-response unit**, such as a cyber-info SWAT team, coordinating with NATO and national intelligence to neutralize propaganda and cyberattacks as they happen, may be established. This could draw from many existing initiatives like the European Digital Media Observatory, centres of excellence, etc. For such a unit to be effective it would need to summon additional national contributions from the most advanced Member States and from the public and the private sectors.
- This unit could be complemented by a coordination mechanism at the EU level to establish a **centralized digital forensics infrastructure** for real-time detection and streamlined responses. This body could build on national efforts like France's Viginum or the Swedish Psychological Defence Agency, preventing Member

States with weaker frameworks from being exploited. It can utilize shared resources and capabilities from all Member States and build on the EEAS Rapid Alert system.

- **Enforcement of digital regulations** like the Digital Services Act (DSA) is uneven, with smaller language markets lacking leverage against big tech. A strong coordination mechanism can level the playing field and improve national enforcement. The EU could offer targeted operational support from existing resources in the Multiannual Financial Framework (e.g., the Digital Europe Programme 2025) to urgently build capacity in national authorities, especially in Central and Eastern Europe, focusing on digital forensics, staff training, and strategic communication. Additionally, a benchmarking assessment should be established to track progress in developing institutional defences against FIMI using common indicators.
- **Local resilience against internal fractures:** The geopolitical strain, war, refugees, inflation, rising extremist parties, fuel local polarization that foreign actors exploit. Civic engagement and independent local journalism need to be reinforced through action at an EU level, by engaging at the grassroots stage and in fringe regions: small communities where disinformation fester. A network of local democracy hubs with funding for real-time counter-narratives and community dialogue could plug this gap, making it harder for Moscow or Beijing to amplify internal rifts.
- **Regaining the tech edge against AI-driven disinformation:** Russia and China are already using AI-generated deep fakes and bots to flood platforms. Countering these threats necessitates going beyond compliance with digital regulations into outpacing adversaries, like some Member States have done. Engaging in positive economic statecraft could foresee investment in cutting-edge AI detection tools and partnerships with tech firms to stay ahead in the game and keep up with the ever-accelerating info war speed.

Media Freedom Support

Media serves as both a critical antidote and frontline defender in hybrid warfare. In a post-truth era of increased political polarisation, a healthy, plural landscape of independent news media outlets serves as an important first-line in the defence of democratic ideals and inoculator against disinformation. However, news outlets continue to collapse, driven in large part by the rise of the commercial internet and social media. The spread of news deserts, areas which are not covered by any local news outlets, are extending across the EU.

A number of actions may be taken to strengthen the news media environment,⁸ ensuring the media can continue to perform its important role for democracy:

- The EU could leverage existing funding frameworks like the European Structural and Investment Funds and adapting instruments such as JEREMIE to unlock equity financing for independent media, especially in underserved regions, ensuring a diverse, innovative, and resilient news ecosystem across the Union. Another instrument to support the news media ecosystem could involve **adapting existing funding instruments from the European Structural and Investment Funds** and adding a thematic priority focused on “Technology Innovation for Media” or “Media Innovation for Democracy” under the Multiannual Financial Framework 2021- 2027.
- The Commission **should pursue regulatory initiatives** encouraging Very Large Online Platforms (VLOPs) and Search Engines (VLSEs) to contribute more actively - such as **through fairer revenue-sharing models or mitigation fees** - to sustain quality journalism. Yet, the enforcement of the Digital Services Act (DSA) must be paired with economic disincentives for non-compliance by VLOPs, which have become instrumental in shaping information markets. The EU should treat disinformation as an economic weapon, deploying targeted sanctions and restricting market access to firms complicit in malign influence campaigns.
- Ensuring citizens have access to reliable, independent journalism also necessitates that access to disinformation and Russian disinformation campaigns is restricted. Since the war in Ukraine, the Kremlin has consistently targeted European citizens with pro-Russian disinformation and propaganda. This has been in support of their broader goal of diminishing the public’s appetite for supporting Ukraine, and reducing the internal cohesion of Europe’s democracies. Thus, the EU has extended its sanctions to 27 Kremlin-backed disinformation outlets, such as RT, Rossiya 1 and Sputnik, suspending their broadcasting activities and licenses.
- However, these outlets are still finding ways to broadcast their disinformation campaigns in Europe, by using mirror- and mushroom sites, social media platforms like YouTube and Telegram, and domestic sites that amplify the Kremlin’s message. The EU, through its Democracy Shield initiative, should extend, and more importantly, **enforce, sanctions on Russia’s local amplifiers within the bloc.**

Next Generation Societal Resilience Measures

Targeted operational support is crucial for civil society organizations (CSOs), researchers, and preventive actors to unify efforts in building societal resilience against disinformation, FIMI, and radicalization. These initiatives should go beyond media literacy and fact-checking programs to address a broad range of audience vulnerabilities and target groups, including algorithmic awareness and societal resilience against information manipulation on the psychological and emotional level. The programming should enable continuous national-level interventions and mobilization, with funding provided at 100% and managed at the EU level to ensure independence and autonomy, particularly from governments with high levels of state capture.

Dedicated funding should support tailored tools for specific audiences, including inoculation and redirect methods, strategic communication campaigns, counter-messaging, and civic education, while fostering AI innovation. The DG HOME ISF-Police Civil Society Empowerment Programme serves as a strong example of funding for civil society-led campaigns against radicalization in the EU, delivering promising results.

The EU could facilitate the establishment of resilience-building interventions and a knowledge hub that produces guidelines and disseminates the latest evidence on effective interventions, including good practices and lessons learned. This knowledge, currently scattered and often reactive, needs to be made accessible to practitioners and policymakers more quickly and in actionable forms. The EU Knowledge Hub on the Prevention of Radicalisation serves as a practical example.

* * *

Russia’s war in Ukraine amplifies its hybrid tactics - disinformation spikes, cyber hits on EU grids, economic pressure via energy. China’s quieter but growing influence (e.g., tech infiltration) compounds the strain. CSD’s state capture framework offers a battle-tested playbook for action. This governance angle reinforces the EDS’s digital and civic focus. Stronger institutions mean less room for Kremlin or Chinese penetration, making democratic resilience more than a buzzword.

⁸ Stoyanova, M., Trifonova, G. and McLaren, R., *Media Financing in Europe: Media Freedom, Market Failure and Instruments for Funding Independent and Pluralist Media*, Sofia: Center for the Study of Democracy, 2024.