GLOBSEC
IDEAS SHAPING THE WORLD

CEDMO
Central European Digital Media Observatory

Co-funded by the European Union

GLOBSEC's Vision for a Stronger European Democracy Shield

Policy Brief

Jana Kazaz, Research Fellow
Vladislava Gubalova, Senior Research Fellow
Dominika Hajdu, Director for Policy & Programming

In response to the European Commission's **open consultation** on the European Democracy Shield (EUDS), GLOBSEC is making its submission publicly available to support a transparent and inclusive policy dialogue. The consultation, launched as part of the EU's efforts to enhance democratic resilience, invited contributions on how to better protect democratic institutions from foreign interference, information operations, and manipulation — and to strengthen electoral integrity, promote civic engagement, and build societal preparedness in the face of evolving hybrid threats.

GLOBSEC's recommendations build on years of experience in countering hybrid threats — particularly in the information domain — as well as in strengthening societal resilience and advancing democratic innovation. Our submission covers all four pillars of the proposed initiative, advocating for the development of EU-wide assessment benchmarks and monitoring mechanisms that could serve both as early-warning tools and as instruments linked to funding conditionality. We also call for reforms to civil society funding schemes to improve accessibility and sustainability, and urge a more comprehensive response to foreign influence operations, expanding both their thematic scope and geographical coverage.

Establish foreign malign influence baselines across the EU

The capacity of Member States to anticipate and counter hybrid threats varies significantly, as demonstrated, for example, by GLOBSEC's 2021 Vulnerability Index.[1] In practice, this enables malign actors to exploit the "weakest links" within the Union and undermine the EU's internal security. Despite increasing efforts at EU level to standardise the taxonomy surrounding foreign malign influence — particularly information manipulation and interference (FIMI) and cyber threats[2] —and to define key areas of hybrid threats[3], no common framework currently exists to establish baselines for resilience against such threats. Although institutional structures differ considerably across Member States and a one-size-fits-all approach is not feasible, those countries generally regarded as successful in building societal and state resilience offer a wealth of best practices. These can be consolidated into a "catalogue" of policies, structural reforms, measures, capabilities, and models of multistakeholder cooperation.

1 https://www.vulnerabilityindex.org/
2 https://www.enisa.europa.eu/sites/default/files/publications/Foreign%20Information%20Manipulation%20and%20Interference%20%28FIMI%29%20and%20Cybersecurity%20-%20Threat%20Landscape.pdf
3 https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/

Such baselines would align with the minimum preparedness requirements and monitoring mechanisms proposed under the Preparedness Union Strategy.[4]

To support the identification of both gaps and strengths, a structured and regular vulnerability assessment across all EU Member States is essential. The existing GLOBSEC Vulnerability Index can serve as a foundation for establishing a more comprehensive assessment framework focused on foreign malign influence.

Recommendations:

- **Develop a set of resilience baselines for Member States** to work towards, building on the minimum preparedness requirements set out in the Preparedness Union Strategy, as well as the recommendations in Sauli Niinistö's report on civilian and military preparedness and readiness.[5]
- **Establish a robust monitoring mechanism** to track progress against these resilience baselines, modelled on the European Semester and the Rule of Law Reports. This cycle should involve EU institutions, Member States, and third parties—including experts, NGOs, and academia—in defining the baselines, outlining the necessary steps for Member States to meet them, and annually monitoring their progress.

Address proxies in FIMI operations

Experts consulted by GLOBSEC for its policy paper[6] outlining EU-specific recommendations on foreign malign influence (FMI) agreed that current efforts tend to focus predominantly on external actors. However, internal proxies – including civil society actors, small companies, information outlets with undisclosed ownership, and individuals – play an equally harmful role in disseminating foreign malign influence within the EU. Evidence of this can be observed in the Romanian presidential election[7], as well as in reports identifying networks of sources, both transparently and non-transparently owned, that regularly republish content from sanctioned Russian state media.

Research by the Alliance for Securing Democracy found *"more than 3,019 unique links on 316 domains in EU search results that linked to content that was identical or a near-duplicate to queried RT articles."*[8] GLOBSEC uncovered a major network of sources regularly republishing content from Kremlin-aligned outlets, including those within the Russia-backed Pravda Network.[9] Additional research by ISD[10] and Science Feedback[11] further substantiates these findings.

Recommendations:

- **Conduct comprehensive monitoring of proxies** that consistently amplify content from sanctioned Russian state media across the EU. This effort should be supported through a public tender open to non-governmental consortia with robust OSINT capabilities. The outcomes of such investigations should inform potential additions to the list of sanctioned foreign individuals and entities under the EU's sanctions regime targeting "destabilising activities against the EU, its Member States and partners."
- **Establish interdisciplinary electoral working groups** to monitor major national elections (parliamentary and presidential) and nationwide referenda starting six months before the vote. These groups should aim to bolster election protection against Russian influence and operate in cooperation with the DSA team and Member States' Digital Services Coordinators. Membership should include representatives from social media platforms active in the respective country, alongside non-governmental experts such as FIMI-ISAC.
- **Develop a systemic approach in the form of**

4 https://webgate.ec.europa.eu/circabc-ewpp/d/d/workspace/SpacesStore/b81316ab-a513-49a1-b520-b6a6e0de6986/file.bin
5 https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf
6 https://www.globsec.org/sites/default/files/2024-08/Shaping%20the%20Next%20EU%20Commission%27s%20Priorities%20-%20Countering%20Foreign%20Malign%20Influence%20chapter.pdf
7 https://www.reuters.com/world/europe/romania-investigates-mercenary-linked-presidential-candidate-after-guns-cash-2025-02-28/
8 https://securingdemocracy.gmfus.org/the-russian-propaganda-nesting-doll-how-rt-is-layered-into-the-digital-information-environment/
9 https://www.globsec.org/what-we-do/publications/global-offensive-mapping-sources-behind-pravda-network
10 https://www.isdglobal.org/wp-content/uploads/2024/02/Two-Years-on_ISD.pdf
11 https://science.feedback.org/sanctioned-but-thriving-how-online-platforms-fail-to-address-the-widespread-presence-of-entities-under-eu-sanctions/

Guidelines under the Digital Services Act (DSA) addressing social media platforms not designated as Very Large Online Platforms (VLOPs) but for which there is substantial evidence of serving as venues for malign influence. These Guidelines should clarify the European Commission's mandate to request data from such non-VLOP platforms in order to assess systemic risks and ensure full compliance with the DSA, including with respect to the number of users in the EU.

Ensure data access for research on systemic risks to democracies

Article 40 of the DSA aims to grant vetted researchers access to data from VLOPs to facilitate the study of systemic risks related to information threats. However, GLOBSEC's 2024 *Access to Data for Researchers*[12] survey found that, in practice, this access remains largely unmet. Researchers continue to face unclear application procedures, inconsistent rules across platforms and Member States, and significant delays. Among 54 experts surveyed across 21 countries, the average rating for their overall access experience was just 4.6 out of 10. Researchers commonly face the following challenges:

- Unclear procedures and eligibility requirements for vetting;
- Limited awareness of available data and unclear definitions of access scope;
- Delays ranging from 2 to 7 months, which undermine time-sensitive research, particularly during pre-election periods;
- Discrepancies across Member States and platforms in how access is granted or interpreted.

None of the respondents reported that Article 40 had meaningfully improved access by late 2024.

Similar concerns were echoed in the EDMO report[13] following the workshop on data access published in May 2024. The report highlighted the same recurring issues: slow or absent responses from platforms, undefined standards for data formats and timelines, and a lack of harmonisation across the EU.

Rather than expanding access, some platforms have reduced the availability of tools previously relied upon by researchers. Notably, in August 2024, Meta discontinued CrowdTangle — a widely used tool for monitoring publicly available content — without offering a fully equivalent alternative. Of the 29 researchers who had used CrowdTangle, 76% reported relying on it daily or weekly; yet only one respondent had found a fully adequate replacement. This move has been widely viewed as a significant setback to transparency efforts.

Recommendations:

- **Introduce organisational-level access with fixed validity:** Replace the current project-by-project assessment model with a system of organisational vetting. Once approved, an organisation should retain access rights for a minimum of two years without the need to reapply. This approach would enhance continuity and ensure research readiness during crises.
- **Guarantee access to machine-readable, high-quality data:** Ensure that researchers are able to download anonymised data in usable formats, including full engagement metrics, content types, advertising expenditure, and algorithmic indicators. Particular attention should be given to restoring functionalities lost with the discontinuation of CrowdTangle.
- **Mandate data-sharing in EU-funded projects:** Require that all EU-funded initiatives focused on digital democracy or online safety include enforceable data-sharing provisions. Platforms participating in such projects must commit to providing relevant data to project researchers — and ideally the broader research community — in a timely manner. This would ensure that EU

12 Access to Data for Researchers_A State of Play.pdf
13 Report-on-EDMO-Workshop-on-Platform-Data-Access-for-Researchers.pdf

funding supports greater data transparency and generates public interest benefits beyond the immediate scope of the project.

Fund and protect civil society organisations as frontline defenders of democracy and information integrity

Civil society organisations (CSOs) are recognised by EU institutions as essential actors in safeguarding democracy.[14] Yet, despite their critical role, CSOs across the EU and its Neighbourhood face an escalating funding crisis and are increasingly targeted for their work.[15]

Many organisations have traditionally depended on support from U.S.-based donors and foundations, including USAID. Recent funding cuts have had a disproportionate impact — particularly in Eastern Europe and the Western Balkans — where up to 80% of NGOs have been directly affected, with some losing nearly all of their funding.[16] As a result, activities have been cancelled and core democratic initiatives placed at serious risk.

Even prior to these external funding cuts, European CSOs faced challenges due to fragmented funding. EU support is dispersed across various programmes (e.g. CERV, Horizon Europe, EDMO grants), which are typically delivered as short-term project-based grants rather than funding that supports core organisational activities.[17] Existing EU funds are limited in scale and often burdened by heavy administrative requirements[18], which smaller grassroots organisations struggle to meet.

An EU-funded survey found that 30% of CSOs identified the "lack of core/infrastructure funding" as a top challenge, while 21% cited the "limited impact" of funding due to its short duration.[19] The European Media and Information Fund (EMIF) exemplifies this gap between demand and available resources: in 2023 alone, EMIF received €29.9 million in funding requests from 100 applicants but had only €4.8 million available for distribution.[20]

While current EU programmes such as CERV, Erasmus+, and Horizon Europe provide essential project-based funding, they seldom offer core or long-term operational support to CSOs. For example, although the CERV programme includes a welcome operating grant scheme, it is primarily designed for EU-level networks and involves a dual application process—framework partnership followed by annual re-application for funding—which requires substantial internal capacity.

Meanwhile, action grants typically run for only 12 to 24 months and often require co-financing. Similarly, regional hubs under the European Digital Media Observatory (EDMO) network—funded through the Digital Europe Programme—are also subject to co-financing requirements. This creates a significant barrier for smaller, yet often highly impactful, national organisations that lack the financial reserves or donor support needed to meet these conditions.

EU initiatives are increasingly positioning CSOs as "strategic partners" in advancing democracy and the rule of law, yet the level of support provided does not reflect this growing responsibility. For example, the Code of Conduct on Disinformation under the DSA envisions substantial CSO involvement in policymaking, fact-checking, and citizen outreach. However, without improved funding for staffing and engagement activities, CSOs are unable to meet these expectations. This leads to an overreliance on unpaid volunteer labour and risks limiting participation to well-resourced organisations from a handful of countries—undermining the inclusive, EU-wide approach that democratic resilience requires.

14 **Civil society under fire: why the EU must act now | EESC**

15 Withdrawal of OSI funds from EU: https://www.reuters.com/world/europe/soros-foundation-limit-eu-funding-new-strategy-internal-email-2023-08-15/, Discontinuation of USAID: **https://balkancsd.net/fallout-of-the-us-funding-freeze-puts-western-balkans-civil-society-under-attack/, EU SEE: https://eusee.hivos.org/the-global-funding-squeeze-on-civil-society-challenges-and-responses/**, Georgia – Law on Transparency and Foreign Funding: **https://eap-csf.eu/articles/battered-but-resilient/ https://apnews.com/article/serbia-usaid-prosecutors-civil-society-probe-02af3400071175e0c4b717fb6b273493**

16 **US aid freeze is leaving a void. Europe must fill it. - Commissioner for Human Rights**

17 The European Court of Auditors (ECA) found that over €7 billion was granted to NGOs in EU internal policies (2021–23) via diverse instruments, yet "there is no reliable overview of EU money paid to NGOs" and information is "published in a fragmented way" - **https://ieu-monitoring.com/editorial/eu-auditors-on-eu-funding-for-ngos-lobbying-and-advocacy-are-not-clearly-disclosed/606085**

18 **https://civilsocietyeurope.eu/wp-content/uploads/2023/12/CERV-mid-term-evaluation-CSOs-proposals.docx-2.pdf**

19 **https://data.consilium.europa.eu/doc/document/ST-14119-2024-INIT/en/pdf**

20 **https://www.eui.eu/news-hub?id=emifs-second-round-of-calls-closes-with-100-applicants**

Alongside these financial constraints, CSOs are increasingly subject to targeted political and regulatory pressure. In some countries, national legislatures have introduced—or proposed—measures that expand administrative burdens and increase state oversight of CSOs, often under the pretext of enhancing transparency or preventing foreign interference.[21] At the same time, CSOs are being portrayed in political and media narratives as destabilising forces—labelled as foreign agents, disruptors of societal cohesion, or drivers of radical change.[22] This trend of instrumentalising civil society as a scapegoat amid broader democratic backsliding highlights the urgent need for institutional safeguards and sustained support mechanisms to ensure the resilience of CSOs and their continued participation in public life.

Recommendations:

- **Reform and expand existing EU operating grant schemes** to enhance civil society access and increase the use of lump-sum funding to progressively eliminate co-financing requirements. The focus should be on providing accessible, flexible, and multi-year support that is minimally bureaucratic and open to both national and cross-border initiatives. Such improvements would enable organisations to sustain core operations, respond to crises, and more effectively leverage project-based opportunities.
- **Further strengthen the Rule of Law mechanism** by incorporating monitoring of CSO sustainability, based on clearly defined benchmarks. Conditionality on access to European funds should be applied as a means to protect CSOs from undue burdens and threats to their work and continued existence.

Limit knowledge fragmentation

While EU funding enables hundreds of civil society projects, their outcomes are often limited in scale or visibility—frequently reported only on shared platforms without broader dissemination. Innovative CSO-led solutions—from local media literacy programmes to fact-checking tools—may prove effective within a specific country or context but are rarely scaled further. As a result, although project activity is abundant, the methodology, applicability, and value for money of such initiatives can be questioned if they remain archived rather than actively utilised.

Not all impactful measures require constant innovation. Many initiatives already trialled and proven effective are well-suited for the coming decade. A shift in focus towards funding projects that identify, consolidate, and scale successful approaches is therefore essential. This model has already been piloted by the EC under Horizon Europe, Pillar II: *Global Challenges and European Industrial Competitiveness*, particularly within Cluster 2: *Culture, Creativity and Inclusive Society*. Projects such as SCALEDEM, for instance, were funded to assess the outcomes of EU-supported civic initiatives and identify democratic innovations with potential for replication across Member States.

Similar efforts should be made to define guiding principles for EU-oriented civic education, which ought to be prioritised. As a fundamental grassroots tool for embedding EU values and principles among citizens, civic education currently suffers from a fragmented landscape—shaped by disparate national curricula and the efforts of CSOs, which often bear the full responsibility themselves. While education remains a national competence, the complementary role of CSOs could be significantly strengthened through the development of a common civic education framework or curriculum at the EU level.

21 Hungary: **https://www.transparency.org/en/press/transparency-international-hungarys-new-bill-threatens-to-end-civil-society-empower-government-persecute-with-impunity#:~:text=Berlin%20%E2%80%94%20A%20new%20legislative%20proposal%20in%20Hungary%2C,organisations%20it%20deems%20a%20threat%20to%20national%20sovereignty**, Georgia: **https://edition.cnn.com/2024/05/13/europe/georgia-foreign-agents-law-explained-intl/index.html**, Slovakia: Slovakia passes law on NGOs amid criticism – DW – 04/17/2025

22 Slovakia: **https://www.politico.eu/article/slovakia-adopts-russian-bill-targeting-ngos/**, Official text of the amendment: 109/2025 Z. z. Novela zákona o neziskových organizáciách poskytujúcich všeobecne prospešné služby | Aktuálne znenie , Georgia: **https://www.bbc.com/news/world-europe-69007465 https://dennikn.sk/minuta/4422327/**

Recommendations:

- **Expand funding for the testing and scaling of existing innovative solutions** developed through EU-funded projects. This approach should be mainstreamed across more EU funding programmes, with mechanisms in place to monitor the efficiency and effectiveness of such projects—specifically assessing whether they contribute to closing knowledge gaps and successfully scaling proposed solutions.
- **Develop a common supplementary EU-oriented civic education curriculum** guide for use by CSOs in their grassroots activities. This would enhance the impact of their work by promoting consistent messaging and methodology, offering practical support, and helping to reduce the current fragmentation in civic education efforts across Member States.

Extend European Democracy Shield to EU Neighbourhood

To effectively counter democratic backsliding and foreign interference in the EU's neighbouring regions—and to prepare candidate countries for eventual full membership—it is essential that Neighbourhood countries are engaged in the European Democracy Shield initiative from the outset. This proactive inclusion is vital for building resilience not only within the EU but also in adjacent states, by addressing vulnerabilities before they can be exploited.

GLOBSEC's *Vulnerability Index 2021* highlights the susceptibility of several non-EU countries to foreign malign influence. For example, Serbia and Montenegro scored 55 and 44 respectively on a 0–100 scale, reflecting notable vulnerabilities in areas such as public attitudes, the political landscape, and the information environment. Persistent risks in the region include state capture, weak rule of law marked by stalled or superficial reforms, and ongoing corruption. In 2024, the decision to allow Russian state-controlled media platforms such as RT to resume operations in the Western Balkans (from Serbia) further increased exposure to foreign manipulation, with potential to undermine EU policies and distort the perception of the enlargement process.[23]

In Ukraine and Moldova, governments are already facing FIMI campaigns attributed to Russia. According to an EEAS report, of the 505 recorded incidents in 2024, 275 occurred in Ukraine and 45 in Moldova.[24]

Recommendations:

- **Include representatives from candidate countries**—including governmental institutions, civil society, and independent experts—in working groups, consultations, and the drafting of EUDS strategies, action plans, and policies. This will strengthen future Member States' ownership of the initiative while shifting the focus away from a solely EU-centred approach.
- **Enhance observation status for candidate countries** in EUDS-related discussions at appropriate institutional levels.
- **Establish interdisciplinary and inclusive electoral working groups** ahead of elections in candidate countries, following the model proposed for Member States (see recommendations above). These groups should involve national authorities, civil society, experts, social media representatives, and relevant EU actors.
- **Incorporate monitoring of compliance with EU-defined resilience baselines** (as outlined above) into the annual Enlargement Reports for candidate countries.
- **Embed resilience-building mechanisms into the conditionality frameworks** of future economic support instruments, such as subsequent editions of the Growth Plan.

23 **https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf**
24 **https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf**

This report has been funded by the Central European Digital Media Observatory (CEDMO) Project, which has received funding from the European Union under the call: DIGITAL-2023-DEPLOY-04, project 101158609. This report reflects the views only of the authors, and the Commission cannot be held responsible for any use that may be made of the information contained herein.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or EACEA. Neither the European Union nor the granting authority can be held responsible for them.