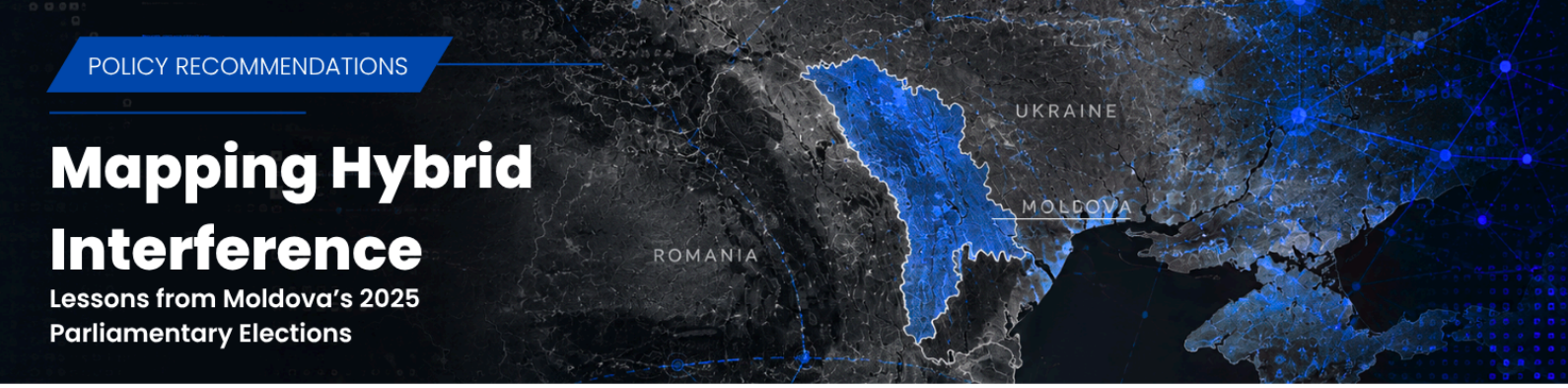

POLICY RECOMMENDATIONS REPORT | JULY 2026

The Foreign Policy Centre

Key Takeaways & Policy Recommendations: Lessons for the UK from a Transnational Influence Battlefield

Author: **Andra-Lucia Martinescu**[1]

The contextual and data-driven analyses tell a clear story: Moldova's 2025 parliamentary election was not merely a consequential national democratic contest but a stress test for Europe's wider resilience to networked interference. One analysis explains the political terrain; the other shows how that struggle was engineered online. Read together, they evidence how hostile influence moves from money to messaging, from local grievance to transnational mobilisation, and from one election to the next.

Some key insights:

- While elections remain national, malign interference (at scale) does not. It persists as a standing infrastructure that operates between electoral cycles, moving across platforms, languages, borders, and communities. Its reach is facilitated by opaque platform algorithms, fragmented oversight, and, increasingly, AI-enabled tools that accelerate content production, translation, targeting and imitation, exponentially. The UK should, therefore, build responses that follow the networks rather than the map.

- Moldova was not simply a target of propaganda. It functioned as an operational theatre for Russia's hybrid strategy, in which the information space was weaponised to shape political choices before voters reached the ballot box (*i.e. participatory deterrence*). Analysis of the online ecosystem over several months preceding the elections revealed not an isolated country-based interference effort, but a regionally integrated information strategy. This hostile strategy simultaneously targeted Moldova, Romania, Ukraine, as well as the European Union (EU), NATO, and other European countries, fused into a single geopolitical battlespace (albeit virtual). Elections are systematically framed from procedural democratic events into externally orchestrated power contests.

---

[1] Andra-Lucia Martinescu is a Senior Research Fellow at the Foreign Policy Centre, specialising in threat intelligence, hybrid operations, conflict analysis and democratic resilience. Her recent work also focuses on how hostile influence, political violence, information manipulation and proxy networks affect vulnerable democracies, particularly across Eastern Europe and the wider European neighbourhood. She has previously held research roles with the British Army's Centre for Historical Analysis and Conflict Research, RUSI, RAND Europe and other institutions, and has provided evidence to the UK Parliament on a number of issues. She is also actively involved in civic-tech, independent electoral monitoring and grassroots democratic initiatives. Andra-Lucia is co-founder of Qriton and The Diaspora Initiative, the latter, an independent Luxembourg-based project working at the intersection of diaspora studies, migration, good governance and democratic participation.

- Under the *Party of Action and Solidarity* (PAS), Moldova experienced its first sustained pro-European alignment between parliament and government since independence. The 2025 parliamentary election preserved this trajectory, but the campaign was marked by intense foreign-backed pressure, proxy mobilisation, and coordinated manipulation at transnational scale. The Moldovan diaspora, estimated at 1.2 million, emerged as a decisive political force and, therefore, also as a strategic target.

- Russia and its vast proxy networks did not rely on a single political vehicle. They appear to have backed or amplified multiple parties and candidates to fragment Moldova's pro-European orientation, confuse voter choices, and insert several channels of influence in the electoral arena. Investigations cited in the reports linked some of these operations to Russian funding, including (but not limited to) support for campaign infrastructure and online dissemination at scale.

- The decentralised behaviour of these influence networks makes them harder to expose and easier to reproduce. Influence is no longer carried only by political parties, state media or paid trolls; it is laundered through NGOs, 'media schools', youth programmes, content creators and self-styled journalists. One example, Evrazia, the Russian-backed non-profit linked to Ilan Shor and sanctioned by the EU and the UK, shows how supposedly civic or educational language can mask an influence pipeline, where youth and young professionals are intensely targeted for recruitment – not only limited to Eastern Europe, but increasingly forceful across Western countries, as well as the US and the Global South.

- The data analysis points to a modular and interconnected interference ecosystem, designed to outlast a single election. Telegram acted as the main coordination and redistribution layer, while TikTok drove engagement exponentially. Overall, the ecosystem spanned and migrated across multiple platforms and the web.

- A distinctive feature of Russian-affiliated activity was the production and dissemination of narratives in multiple languages through channel and account spin-offs, and often with near-identical semantic structures. Channels or accounts that appear to operate from the UK or Germany are likely controlled by actors/units elsewhere, using VPNs, spoofed metadata, or leased digital infrastructures to shield themselves through plausible deniability.

- This multilingual architecture becomes relevant for the UK, with anglophone amplification as a distinct feature. For instance, narratives around alleged voter suppression in Transnistria were picked up by English-language channels, linked in the report to figures with direct connections to Russian state media and influence operations. Such channels help launder Russian-origin claims into wider English-speaking audiences, giving them a veneer of independent commentary before they are recirculated into European, diasporic, and domestic political spaces.

- Disinformation networks repeatedly target civil society organisations, independent media or watchdog civic groups as corrupt agents of foreign interests, collapsing all institutional checks into a single hostile 'system'. This tactic is designed to isolate democratic actors, discourage scrutiny, and normalise conspiracy narratives as common sense.

- Diaspora communities are not merely overseas constituencies in a procedural sense but have increasingly become vectors of cross-border information environments. This aspect makes them both a democratic asset and a strategic target: they can decisively impact elections, but they can also be exposed to demobilisation, polarisation, and political radicalisation.

Narratives travel transnationally and often under the radar of response and prevention efforts, through families, platforms, community groups, churches, influencers, and local politics, in both countries of origin and residence.

- In the 7th May UK local elections, 100 Romanian-origin candidates stood; half ran on the Reform UK ticket. This may seem paradoxical if viewed outside the more insidious dynamics of transnational populist/extremist circulation, where anti-establishment, anti-EU, 'sovereign' and anti-migration narratives can be repackaged across contexts, even when they sit uneasily with the lived experiences of migrant communities themselves. It should not be read as evidence of malign activity, but as a cautionary tale that populist and far-right platforms in Moldova, Romania and other European localities (the UK notwithstanding) increasingly draw from a common political grammar, adapting the same emotional cues to different national settings: betrayal, loss of control, cultural displacement, institutional distrust and the promise of restoration.

Recommendations for the UK:

- As a **strategic priority**, the UK should treat democratic legitimacy as a national security asset. Moldova shows that hostile influence is not an episodic campaign tactic but a permanent architecture for degrading trust, fragmenting coalitions and making democratic choice feel futile. The UK response must, therefore, be equally permanent, transnationally aware and network-focused.

- **Make transnational influence a core resilience test**: UK democratic security should move beyond the domestic/foreign divide. Hostile state-sponsored networks operate fluidly through language spaces, communities, platforms, financial pipelines and political identities that transcend borders. Risk assessments by the Cabinet Office, Electoral Commission, Ofcom, and local authorities should therefore ask not only "is this content legal?" but "which infrastructure is making this particular message/narrative travel, and who benefits?"

- **Beyond content**: The UK should also treat hostile influence as a capacity-building ecosystem, not only a content problem. Sanctions, platform enforcement, political finance scrutiny and civil society support should also be designed to disrupt recruitment pipelines, media-training fronts posing as legitimate journalism, and cross-border amplification networks before they mature into electoral assets.

- **Risk mapping and mitigation**: The UK should develop a dedicated democratic resilience risk index to track permanent influence infrastructures, not only acute election threats. This would complement the National Risk Register, the Defending Democracy Taskforce and the Foreign Influence Registration Scheme (FIRS) by measuring slow-burn risks to democratic legitimacy; e.g. opaque funding, proxy outlets/hubs, AI-enabled amplification suffocating online public debate, legal intimidation, transnational relay networks, etc.

- **Platform accountability**: The UK should not rely on 'proactive' platform cooperation nor leave democratic integrity to platform discretion. The Online Safety Act affords Ofcom powers to address illegal online harms, including foreign interference, but it does not yet constitute a dedicated election-integrity transparency regime comparable to the EU's Digital Services Act's systemic risk framework. Ofcom and the Department for Science, Innovation and Technology (DSIT) should develop enforceable election and crisis protocols that require platforms to preserve and disclose network-level evidence (i.e., tackling the infrastructure of

inauthentic coordination that mimics organic consensus), with secure access for regulators, electoral authorities, and vetted researchers.

- **Build resilience through bilateral and regional partnerships**: The UK should embed democratic resilience and information integrity provisions into its existing bilateral strategic partnerships. Existing frameworks with Moldova and Ukraine increasingly address hybrid threats, cyber resilience, and foreign information manipulation, but equivalent provisions are not consistently embedded in strategic partnerships with other exposed European states, such as Romania. These enhanced frameworks should cover shared threat mapping, sanctions coordination (with the EU), platform evidence-sharing, journalist protection, political finance risks, and monitoring.

- **Protect civic trust as critical infrastructure**: Journalists, watchdogs, researchers, and community organisations should be treated as part of the UK's early-warning system. Anti-SLAPP (Strategic Lawsuits Against Public Participation) protections, secure reporting channels, and targeted support for investigative capacity should be strengthened because hostile networks often attack civil society first in a bid to weaken the civic tissue that exposes manipulation, verifies facts, protects vulnerable communities, and sustains public trust.

- **Close political finance loopholes**: Parliament should strengthen the UK's defences against opaque and foreign-linked money. Existing safeguards remain fragmented across the Electoral Commission, police and other agencies, with no dedicated national unit responsible for political finance enforcement. The government should adopt the recommendation to create a specialist Political Finance Enforcement Unit, bringing together the Electoral Commission, police, National Crime Agency (NCA), HMRC and other agencies' expertise.[2] This should be paired with 'know your donor' duties, tighter rules on company donations and unincorporated associations, beneficial ownership disclosure, and restrictions on crypto donations, and clearer checks on the original source of funds behind major donations.

To conclude, for far too long, the UK's openness, legal sophistication, and financial depth have also made it an attractive destination for oligarchic wealth, mercenary and opaque networks seeking access, protection or influence. Moldova's experience shows why this cannot be treated as a narrow financial integrity issue. The same networks that shelter assets or reputations can also sustain malign influence, fund proxies and weaken democratic choice across borders. For the UK, recognising these connections becomes a duty of care: to protect the integrity of its financial, legal, political and civic systems, and to ensure these are not used as permissive spaces from which hostile influence can shelter, regenerate or project power into more exposed democracies.

Disclaimer: The views expressed in this publication are those of the individual author and do not reflect the views of The Foreign Policy Centre.

[2] Joint Committee on the National Security Strategy, Political finance and foreign influence, Third Report of Session 2024-26, UK Parliament, March 2026, https://publications.parliament.uk/pa/jt5901/jtselect/jtnatsec/720/report.html