Conférence européenne des **Présidentes et Présidents de Parlement**
European Conference of **Presidents of Parliament**
Rome, 15-16 octobre 2026 / 15-16 October 2026

Resilient democracies: united against hybrid threats

Background document

"Our vulnerabilities are being weaponized by foreign powers — amplified by technology and artificial intelligence, financed through cryptocurrency, disguised in democratic language. These are no longer attacks on institutions — they are assaults on our very sovereignty."
Maia Sandu, President of the Republic of Moldova, 2025

"Security starts with democracy",
Alain Berset, Secretary General of the Council of Europe, 2026

"Today, Europe's security is being undermined not only by military means, but by hybrid threats as well – from disinformation and energy blackmail to cyberattacks. Defending our democratic security is our shared responsibility."
Ruslan Stefanchuk, Speaker of the Verkhovna Rada, 2025

1. Introduction

1. In today's geopolitical environment marked by growing instability and uncertainty, the traditional concept of **security** is undergoing a profound transformation. Hybrid threats proliferate and have become increasingly sophisticated, amplified by technological advances. Hostile states and non-state actors exploit the openness and vulnerabilities of democratic societies to sow division, deepen polarisation and undermine public trust in institutions and democratic processes.

2. Hybrid threats are not isolated incidents. Rather, they form part of a deliberate strategy aimed at weakening democratic resilience and destabilising societies from within. As the Council of Europe has already pointed out, "Foreign interference is not a marginal or short-term phenomenon, but a structural challenge to democratic and national security that requires careful legal, policy and institutional responses, grounded in respect for human rights, democracy and the rule of law."[1]

2. A multidimensional threat

3. **Foreign Information Manipulation and Interference (FIMI)** is the most common and impactful type of hybrid threat. It can take the form of **disinformation campaigns**, which are co-ordinated efforts to disseminate false or misleading information, particularly during periods of political unrest or elections. Propaganda, bot networks and fake news are deployed with precision to polarise and mislead. Another form is **social media amplification**, whereby algorithms and bot networks increase the visibility of divisive or false content, thereby outpacing objective information. There are also cases of targeted messaging aimed at vulnerable groups, parties or communities, designed to influence opinions or provoke discord (**targeted influence operations**). Research consistently shows that women in public life – politicians, journalists, and civil society leaders – are disproportionately targeted by such operations, which deploy gendered abuse, sexualised content and reputation attacks as tools of political intimidation. This constitutes not only a human rights violation but a structural threat to democratic participation, with documented chilling effects on women's willingness to stand for office or engage in public debate.

4. While FIMI is not a new phenomenon per se, digital technological advances have introduced a new dynamic. Online service providers, including social media platforms, now enable the rapid, large-scale dissemination of manipulated content in ways that were previously impossible. Artificial intelligence (AI) further increases the speed, reach, and sophistication of such activities. The World Economic Forum ranks misinformation and disinformation as among the most severe short-term risks, second only to geoeconomic instability.[2]

---

[1] Council of Europe feasibility study on foreign information manipulation and interference (FIMI), CM/Inf(2026)18.
[2] The Global Risks Report 2026, World Economic Forum.

5. **Hybrid threats** often target critical infrastructure essential for public safety, security, and economic stability. These threats can include sabotage, cyberattacks, signal jamming, drone incursions, and other illicit activities – often carried out by individuals or local proxies deliberately recruited or manipulated for this purpose. Such actions aim to test, disrupt, or undermine the resilience of democratic societies.

6. Recent experience shows that a wide range of actions – from personal data theft to the disruption of essential services, migration flows, energy, food supplies, or trade – can be weaponised. This list is not exhaustive.

3. Countering FIMI

7. FIMI is a core component of the arsenal of hybrid threats targeting democratic societies, yet gaps and structural challenges in responding to it persist to this day. A major issue is the lack of a shared understanding of FIMI: countries have different definitions, thresholds, and perceptions of its links to broader hybrid threats. Institutional capacities also vary considerably. While some states have specialised structures and co-ordination mechanisms, others rely on fragmented arrangements, which affects the consistency and effectiveness of responses.

8. Policy approaches are often fragmented across sectors such as the media, cybersecurity, governance, and criminal law, which limits coherence and cross-sector co-operation. The absence of common methodologies, indicators, or benchmarking tools makes assessing resilience difficult, and pan-European exchanges of good practices are limited.

9. As FIMI is inherently cross-border, differences in legal frameworks, threat perceptions, information-sharing practices and institutional capacities can complicate international co-operation. Further challenges arise from engagement with digital platforms, the rapid development of AI and the manipulation of emerging technologies.

10. Financial and corruption-related vulnerabilities can facilitate interference activities. Differences in criminal law frameworks and legal definitions can hinder investigations and judicial co-operation. Finally, while existing international legal instruments are relevant, they were not specifically designed for FIMI, which leads to uneven implementation and effectiveness across member States.

11. Recognising the prevalence and disruptive impact of FIMI, as well as the need for a co-ordinated response, has compelled European organisations to devise robust strategies.

12. The Council of Europe has adopted a comprehensive approach through the conceptualisation of its **New Democratic Pact for Europe**,[3] which places significant emphasis on defending democracy against FIMI.[4] Following a thorough feasibility study on a potential Council of Europe instrument on FIMI, the Committee of Ministers instructed the Secretary General to submit proposals for negotiating an appropriate legal instrument, including a possible framework convention, at its Chisinau meeting in May 2026. This instrument would address FIMI based on the Council of Europe's standards and expertise.[5]

13. Furthermore, the European Union has developed a comprehensive approach to countering FIMI, combining political co-ordination, operational analysis, regulation, and rights protection. Through the **European Democracy Shield**,[6] the EU seeks to strengthen situational awareness, democratic institutions, media freedom, and societal resilience. The European Centre for Democratic Resilience[7] supports the sharing of expertise and best practices, while the FIMI Toolbox[8] includes strategic communication, public attribution, diplomatic engagement, support for independent media, media literacy initiatives, early-warning mechanisms, international co-operation, and, where necessary, sanctions.

[3] Building a Resilient Europe – The New Democratic Pact for Europe.
[4] Report 2026 - Secretary General.
[5] CM decision.
[6] European Democracy Shield.
[7] European Centre for Democratic Resilience – European Commission.
[8] A practical toolkit for detecting, assessing, and responding to Foreign Information Manipulation and Interference (FIMI).

4. Elections as critical infrastructure

14. Elections are critical infrastructure in democratic systems because they are the fundamental way in which the legitimacy of institutions is established, and democratic rights exercised. Therefore, the integrity, legitimacy and public trustworthiness of electoral processes are essential to the stability and resilience of democratic governance.

15. In recent years, elections have increasingly become prime targets of hybrid threats. In some cases, foreign interference has been directly documented; in others, the electoral environment has been affected by a wider ecosystem of disinformation, manipulative online campaigning, illicit influence, cyber threats and domestic information manipulation. These activities do not necessarily aim to change the final result of the elections but to weaken public trust in the fairness and legitimacy of the electoral process itself.

16. Recent PACE election observation missions have noted unprecedented levels of foreign interference in elections, taking different forms: economic pressure (such as restricting energy access and threatening supply chains), covert political financing (including supporting proxy groups and vote-buying networks), and information warfare (such as spreading disinformation and deepfakes, and using targeted messaging and polarising narratives on social media platforms). Notably, deepfake technology has been deployed overwhelmingly against women candidates and elected representatives – in the form of fabricated sexual imagery and false scandal narratives – constituting a distinctly gendered form of electoral interference whose chilling effect on women's political participation deserves explicit recognition and targeted legal remedies.

17. Hybrid tactics often combine cyberattacks, economic coercion, illicit funding and campaign manipulation. These tactics aim to sway public opinion and exert long-term geopolitical leverage. Observers also reported the use of artificial intelligence to generate manipulative content, posing risks of both foreign and domestic origin. Unregulated online campaigning and a limited institutional response increased vulnerability, particularly where rapid, co-ordinated countermeasures were lacking.

18. Several cases illustrated the challenges posed by delayed or inconsistent inter-agency co-ordination, opacity in third-party campaign financing and difficulties in monitoring digital threats. While direct evidence of outcome manipulation was rare, the persistent use of hybrid means to manipulate information and FIMI remain significant risks, even in countries with robust democratic institutions.

5. Protecting the integrity of elections from foreign interference: lessons learnt

19. In order to protect elections from foreign interference, a combination of cybersecurity, transparency and societal resilience is required. Experience in Europe shows that the most effective approaches combine legal safeguards, technical protection and measures to strengthen public trust.

20. Key lessons include securing election infrastructure through robust **cybersecurity** measures, continuous monitoring, contingency planning and transparent audit and recount procedures. **Regulating foreign influence** through an appropriate legal framework and introducing stricter **campaign finance rules and transparency requirements for political advertising** help prevent covert external interference. As foreign actors increasingly target voters rather than voting systems, governments must also combat disinformation by providing **rapid fact-checking** services, engaging in strategic communication and co-operating with digital platforms.

21. **Independent media outlets and civil society organisations** play a vital role in exposing interference and strengthening democratic resilience. Additional safeguards are required for emerging technologies, particularly AI, including transparency, human oversight and risk-mitigation measures. In this context, the new Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law establishes a general obligation for states to protect democratic processes. This relates, among other things, to the risks posed by AI to the participation in democratic processes through free and fair elections.[9]

[9] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225), Article 5.2. See also PACE Opinion No. 303 (2024).

22. The European Court of Human Rights has recognised that member States may be required to adopt **positive measures to protect the integrity of electoral processes** in the event of a real risk of hostile foreign interference. States should not remain passive when faced with evidence that their democratic processes are under threat.[10]

23. Examples from Europe, such as **Estonia**'s secure digital voting systems and enhanced EU co-operation ahead of the **2024 European Parliament elections**, demonstrate the importance of co-ordinated action. The **Republic of Moldova** is a particularly relevant case study, having faced sustained foreign information manipulation and interference combining disinformation, illicit financing, cyberattacks, proxy mobilisation and attempts to undermine trust in electoral institutions. Recent assessments emphasise the need for stronger institutional co-ordination, greater transparency in campaign financing, effective platform oversight, and support for media literacy and independent journalism.

24. The central lesson is clear: securing voting systems is not enough to ensure election integrity; the wider information environment must also be protected.

6. A whole-of-society approach: harnessing collective strength

25. Effective resilience against hybrid threats depends on three interrelated dimensions: institutional, digital and societal resilience.

26. A whole-of-society approach to countering hybrid threats recognises that governments cannot safeguard democracy and security alone. Effective resilience requires co-ordinated action across public institutions, civil society, the private sector, independent media outlets, academic institutions and citizens. Civil society organisations promote accountability, strengthen community resilience and enhance media literacy. Private companies, particularly those in the technology and cybersecurity sectors, play a critical role in detecting and mitigating cyberattacks, disinformation and other forms of manipulation. Independent media outlets provide reliable information and help to counter false narratives, while researchers and academic institutions contribute evidence-based analysis, innovation and fact-checking. Women-led and feminist civil society organisations occupy a particular position in this landscape: they are both frequent targets of foreign-backed interference and smear campaigns and experienced early-warning actors whose expertise in identifying and documenting co-ordinated harassment and disinformation remains underutilised by formal institutions. A genuinely inclusive whole-of-society approach must actively engage these organisations as partners, not merely as beneficiaries of protection.

27. This approach is implemented in practice through initiatives such as journalist training, media and digital literacy programmes, information-sharing mechanisms and cross-sector crisis response networks. This kind of co-operation fosters resilience to hybrid threats while ensuring that responses remain democratic, rights-based and adaptable.

28. Public awareness and civic preparedness are essential components of democratic resilience. Citizens are often the primary targets of hybrid threats, particularly disinformation and influence operations. Strengthening media and digital literacy alone is not sufficient; governments, parliaments, educational institutions and civil society should work together to develop sustained public awareness campaigns that help citizens recognise manipulation, understand how hybrid threats operate and respond critically to misleading information. Such programmes must also be gender-sensitive. Significant gaps persist in women's access to digital skills, online safety knowledge and the confidence to participate in digital public spheres – gaps that hostile actors actively exploit. Literacy initiatives that do not account for these structural inequalities will reach only part of the population they aim to serve.

29. **Finland's comprehensive security model** uses a whole-of-society approach, involving government, businesses, NGOs, academia, and citizens in co-ordinated security efforts to counter hybrid threats. This system emphasizes information sharing, joint planning, and training to ensure preparedness at every level, with a focus on citizens' psychological resilience and household readiness. Public-private co-operation is especially strong in securing supply chains and critical infrastructure. Finland also enhances resilience through media literacy, supporting independent media, and collaboration between authorities and media to fight disinformation. Co-ordination is led by central government bodies like the Security Committee, while education and networking across sectors improve crisis response and preparedness.

[10] European Court of Human Rights, *Bradshaw and Others v. the United Kingdom*, application no. 15653/22, 22 July 2025.

30. Finland's approach shows that resilience depends on both **preparedness and response**. Democracies must respond rapidly to hybrid threats and also invest in preventative measures to minimize vulnerabilities before crises arise. This dual strategy involves strategic foresight, scenario-based exercises, public preparedness programs, early-warning systems, and strong institutional co-ordination. These elements should work alongside crisis-management and response capabilities to create a comprehensive and robust defence against hybrid threats.

7. The role of national parliaments

31. National parliaments play a crucial role in countering foreign interference and bolstering democratic resilience in the face of hybrid threats. As representative institutions at the heart of democratic systems, they are instrumental in adopting, refining and overseeing policies that protect democratic processes and institutions. Their active engagement enhances the legitimacy and effectiveness of measures aimed at addressing foreign influence and manipulation. Evidence suggests that gender-balanced parliaments are more resilient to populist pressure and democratic backsliding, and that the underrepresentation of women in security and defence committees constitutes a structural gap in parliamentary oversight of the very threats this paper addresses. Finland — cited above as the model for whole-of-society resilience — also ranks among Europe's leaders in women's parliamentary representation, a correlation that warrants deliberate attention when drawing lessons for other member states.

32. One of the primary responsibilities of parliaments is **legislative activity**. They review and adapt existing laws in response to evolving hybrid threats, ensuring that new measures remain consistent with democratic values, fundamental rights and the rule of law. Parliaments are, therefore, encouraged to debate and ratify legislative initiatives, including those proposed under the EU Defence of Democracy Package, as well as international treaties developed under the auspices of the Council of Europe, in particular the Framework Convention on Artificial Intelligence.

33. Parliaments also contribute to this through **policy innovation**. They help build stronger safeguards against external interference by developing and discussing strategies related to cybersecurity, electoral integrity, and transparent communications. Another key aspect of their work is promoting transparency and accountability, particularly in political finance and advertising.

34. At the same time, addressing foreign interference requires a delicate balance. Measures to counter undue **foreign influence** or to enhance transparency must align with human rights standards, particularly those safeguarding freedom of expression, association, assembly, and freedom of thought, conscience, and religion. Overly restrictive laws designed without adequate attention to this balance risk stifling legitimate democratic activity and freedom of expression, chilling civil society engagement, or being misused for political purposes.

35. Beyond legislation, parliaments serve as a **bridge between citizens and public institutions**. By engaging with civil society, independent oversight bodies and the general public, they facilitate dialogue and contribute to raising awareness of hybrid threats and strengthening democratic culture. They also play an **international role**, co-operating with and exchanging best practices with partners in the Council of Europe, the European Union, and other international organisations.

36. National parliaments can foster unity, accountability and trust by combining legislative action, oversight, public engagement and international co-operation. This ensures that resilience against foreign interference becomes a **cross-party priority and a shared societal commitment**.

8. Conclusions

37. Due to their multinational nature, hybrid threats blur the line between peace and conflict. Faced with these mounting security challenges, European democracies must strengthen their capacity to identify hybrid attacks and to defend themselves. Their most powerful asset lies in their unity. Building resilience requires active engagement from all members of society, as well as the fostering of a cohesive international front among partners committed to safeguarding freedom, justice, democracy, and human rights. In an era of growing geopolitical tensions, **unity is the bedrock of democratic resilience and the most effective defence against those who seek to undermine it.**

Questions for discussion

- How can democracies balance countering FIMI with protecting freedom of expression?
- How can the Council of Europe co-operate with others than member states in developing political, social, and technical resilience against FIMI?
- How can national parliaments share their experience with foreign influence legislation?
- What lessons can be learnt from the experience of European states who successfully countered FIMI to protect electoral integrity?
- What mechanisms can strengthen co-ordination between local, national, and international actors to respond rapidly to hybrid threats?
- How can civil society and the private sector be involved in institutional efforts to strengthen resilience?
- What indicators can be used to measure democratic resilience in the face of hybrid attacks? Can the Parameters for the Application and Implementation of the Reykjavík Principles for Democracy play a role?
- How should democracies respond to AI-driven disinformation that outpaces traditional fact-checking?
- How can AI be used to counter hybrid threats?
- In what ways can national parliaments foster greater citizen engagement and trust during periods of heightened instability and polarisation?
- What initiatives can be undertaken to strengthen inter-parliamentary dialogue against foreign interference?
- How can national parliaments support the New Democratic Pact for Europe?
- What initiatives can be developed to foster greater co-operation between like-minded international organisations in countering hybrid threats?
- How can counter-FIMI strategies specifically address the disproportionate targeting of women politicians, journalists and civil society leaders through gendered disinformation, deepfakes and online harassment, and what legislative or institutional measures are needed to close the current protection gap?

Appendix: key reference documents and webpages

Parliamentary Assembly of the Council of Europe

- Resolution 2593 (2025) "Foreign interference: a threat to democratic security in Europe"
- Resolution 2622 (2025) "Russia: new threats to European democracies"
- Resolution 2636 (2026) "Elections in times of crisis"

Council of Europe

- Report 2026 - Secretary General
- Building a Resilient Europe - The New Democratic Pact for Europe
- Council of Europe feasibility study on foreign information manipulation and interference (FIMI)
- Parameters for the Application and Implementation of the Reykjavík Principles for Democracy (CM(2024)48-final)
- European Court of Human Rights, *Bradshaw and Others v. the United Kingdom*, 22 July 2025
- Parliamentary conference – Elections in times of crisis (Bern, 9-10 May 2023)

European Union

- Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, European Democracy Shield: Empowering Strong and Resilient Democracies, JOIN/2025/791 final
- 3rd EEAS Report on Foreign Information Manipulation and Interference Threats
- Best Practices in the whole-of-society approach in countering hybrid threats