Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. …
5 March 2025

Committee on Political Affairs and Democracy

Foreign interference: a threat to democratic security in Europe

Rapporteur: Ms Zanda KALNIŅA-LUKAŠEVICA, Latvia, Group of the European People's Party

Draft report[1]

[1] Reference to committee: Doc.15605, Reference 4693 of 25 November 2022.

A. Draft resolution[2]

1. Intentional, covert and manipulative interference by foreign powers, their proxies or private actors jeopardises security, democratic values, and governance across Europe. This foreign interference aims to undermine sovereignty, destabilise political systems, weaken public trust, and distort democratic processes. These orchestrated efforts continue to increase in volume and velocity, targeting the foundations of European societies and attempting to exploit democratic principles as systemic vulnerabilities.

2. The Parliamentary Assembly recognises foreign interference, in its many forms, as a substantial and persistent threat to democratic security. The Parliamentary Assembly condemns deliberate and systematic efforts by foreign actors to undermine electoral and democratic processes and institutions.

3. The Assembly notes the escalation in hostile interference originating from the Russian Federation following the beginning of its full-scale war of aggression against Ukraine. This has been underlined by the extensive efforts to spread disinformation, covertly fund political campaigns, and buy votes in the Republic of Moldova's presidential election and constitutional referendum of 20 October 2024. Furthermore, the disruption of Romania's presidential election of 24 November 2024 due to the manipulation of digital technology and artificial intelligence conducted from abroad highlights the urgent need to fortify democratic processes against hostile threats and co-ordinated inauthentic behaviour online.

4. This activity forms part of a wider pattern that has included attempts by the Russian Federation to interfere in electoral processes and referenda across the continent over the past decade, with evidence of covert interference during the 2016 Brexit referendum in the United Kingdom, the 2016 United States presidential election, the 2017 coup d'etat from Catalonian regional government leaders against the Spanish constitutional order, the 2017 French presidential election, the 2024 Romanian and Moldovan presidential elections, and in German politics.

5. Democracies must defend themselves against the threat posed by foreign interference as part of an adaptation to this increasingly hostile international environment where the principles of sovereignty, self-determination and democracy are under attack. The resilience of democratic institutions is crucial in countering these dangers and ensuring that the values of human rights, democracy and the rule of law prevail.

6. At the same time, addressing foreign interference requires a delicate balance. Measures to counter undue 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 risks stifling legitimate democratic activity and freedom of expression, chilling civil society engagement, or being misused for political purposes.

7. The Assembly underscores that building resilient societies with strong democratic institutions, an active and informed civil society, and transparent governance is the most effective way to counter foreign interference and ensure democratic security.

8. Efforts to enhance the transparency in public life to combat foreign interference must be implemented in a manner that respects and upholds the freedoms and autonomy of civil society organisations. While safeguarding national interests is crucial, transparency measures should not be used as a pretext for imposing undue restrictions on civil society actors, who play a fundamental role in fostering democratic values, public accountability, and social cohesion.

9. The Assembly notes that the Council of Europe has a wide range of international standards and guidelines aimed at strengthening democratic resilience that are relevant for combatting foreign interference. These include measures to ensure transparency and accountability in public life, international standards and guidelines for political party funding and elections, and strategies to combat disinformation. These tools are further strengthened by the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225, "the Vilnius Convention") which aims to fill legal gaps that may result from rapid technological advances.

10. The Assembly recalls that, at their Fourth Summit in Reykjavik in 2023, the Heads of State and Government of the Council of Europe reiterated their commitment to countering disinformation that posed a threat to democracy and peace in a manner compatible with international law and the right to freedom of

[2] Draft resolution adopted by the committee on 5 March 2025.

expression and freedom of opinion, as well as the commitment to taking appropriate measures against interference in electoral systems and processes.

11. The Assembly stresses the need for comprehensive and holistic strategies to combat the use of multiform foreign interference tactics. A whole-of-society approach that includes parliaments, governments, government agencies, local authorities, private enterprises, journalists, civil society and citizens is encouraged to foster societal resilience and counter foreign interference operations.

12. In light of the threat to democratic security posed by foreign interference, the Assembly calls on member States to:

12.1. integrate foreign interference threats into national security frameworks that recognise the interconnected nature of hostile cyber, economic, political and information activities;

12.2. secure democratic institutions, critical infrastructure, and electoral systems against cyber threats;

12.3. enhance co-ordination between security agencies both nationally and internationally to detect and counter foreign interference activities;

12.4. consider updating laws and regulations to incorporate foreign interference offences for covert conduct on behalf of foreign actors aimed at having a manipulative interference effect.

13. As part of a whole-of-society approach to enhance resilience, reinforce public trust, and safeguard institutional integrity, the Assembly calls on member States to:

13.1. promote digital and media literacy initiatives aimed at countering disinformation and building resilience among citizens to empower citizens against manipulation;

13.2. introduce digital media literacy education into national curricula from an early age to develop essential critical thinking skills for exercising judgment, evaluating the credibility of information sources, identifying biased or misleading content, and for critically and effectively engaging with information online;

13.3. in line with its Resolution 2192 (2017) “Youth against corruption”, devise appropriate empowerment strategies to raise young people’s awareness and understanding of corruption and the ways it undermines democratic societies;

13.4. encourage and support pre-bunking and fact-checking systems, and partnerships with independent media organisations and civil society to counteract false narratives without undermining freedom of expression;

13.5. continue efforts to protect journalists, safeguard press freedom, and to fund and promote media pluralism and independence;

13.6. in line with Assembly Resolution 2552 (2024) “Strengthening democracy through participatory and deliberative processes”, foster more robust civic engagement with deliberative technologies and participatory processes.

14. In light of the risks presented by disinformation as a strategic foreign interference tool to distort realities, divide societies, and weaken democracies, the Assembly:

14.1. welcomes the United Nations Global Principles for Information Integrity Online as a global initiative to foster healthier and safer information spaces, and calls for consultations with the public and with private industry on steps that may be taken to implement its principles;

14.2. calls on Council of Europe member and observer States who have not yet done so to sign and ratify the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225, “the Vilnius Convention”) and ensure its implementation with due regard to the impact of artificial intelligence technologies on the production and dissemination of disinformation and illegal propaganda;

14.3. calls on member States to increase expertise and technical capabilities for combatting disinformation online and to address emerging threats posed by artificial intelligence;

14.4. calls for member States to explore the development of information verification systems to safeguard online communities against deceptive artificial intelligence election content;

14.5. calls on online platforms to provide clear policies on political advertising, algorithmic amplification, and the removal of harmful content or disinformation, while safeguarding the freedom of expression.

15. In light of hostile actor attempts to interfere improperly or illicitly in democratic decision-making processes, the Assembly:

15.1. reiterates its condemnation of massive covert Russian funding of political parties and politicians in democratic countries to try and interfere in their democratic processes;

15.2. calls on member States to ensure legislative and policy frameworks that protect against interference in electoral systems, and to carry out comprehensive investigations into allegations of interference in elections and referenda;

15.3. calls on member States to review and enhance national frameworks governing financial contributions to political parties, advertising and electoral campaigns to mitigate the risk of inappropriate or illicit foreign financial interference;

15.4. in line with its Resolution 2406 (2021) “Fighting corruption – General principles of political responsibility”, calls on national governments to enhance measures for preventing corruption and, in line with recommendations of the Group of States against Corruption (GRECO), to adopt and update codes of conduct for all holders of public office;

15.5. encourages member States to explore measures that increase the transparency and integrity of legitimate foreign influence activities;

15.6. encourages member States to consult at an early stage with the European Commission for Democracy through Law when developing public governance tools to strengthen the transparency and integrity of foreign influence activities.

16. In light of the need for collective action to respond to the global challenge posed by foreign interference, the Assembly:

16.1. stresses the importance of co-operation among Council of Europe member States to address foreign interference as a shared threat. In this regard, it advocates for closer collaboration with the European Union, the Organization for Security and Co-operation in Europe (OSCE), relevant NATO expertise and other international organisations in developing co-ordinated responses;

16.2. encourages support to multi-partner rapid response initiatives to identify and respond to diverse and evolving threats to democracies, including through sharing information and analysis, and identifying opportunities for co-ordinated responses;

16.3. supports the use of targeted and co-ordinated sanctions against individuals, entities and state actors engaged in foreign interference including election meddling, media manipulation, illicit funding and cyberattacks;

16.4. calls for strengthened legal avenues to hold foreign and domestic actors accountable for facilitating interference in democratic processes;

16.5. encourages member States to assess the feasibility of developing a broad-based, operational, non-binding definition of foreign interference to enhance co-ordination in countering related threats and to strengthen clarity on legitimate influence activities of member States;

16.6. welcomes the Assembly’s establishment of the Parliamentary Alliance for Free and Fair Elections as an important step for addressing emerging challenges that threaten electoral integrity, enhancing co-operation with national and international partners on electoral matters, and for promoting Council of Europe reference standards in electoral matters.

B. Draft recommendation[3]

1. The Parliamentary Assembly, referring to its Resolution xxxx (2025) “Foreign interference: a threat to democratic security in Europe” underscores that intentional, covert and manipulative interference from foreign powers or their proxies is a continued threat to the core pillars of democratic security shared by the member States of the Council of Europe.

2. Such interference seeks to undermine electoral processes, erode public trust in democratic institutions, national unity, and distort political decision-making. The most glaring example of this threat is the escalation in hostile interference originating from the Russian Federation following the beginning of its full-scale war of aggression against Ukraine, which the Assembly firmly condemns.

3. The Assembly stresses that a co-ordinated and comprehensive response is required to counter the threat of foreign interference effectively, and advocates for closer collaboration with the European Union, the Organization for Security and Co-operation in Europe (OSCE) and other international organisations.

4. In addition, the Assembly emphasises that free and fair elections are the cornerstone of democratic societies. Independent and transparent electoral processes are necessary for both citizen’s trust in public institutions, and for the competitiveness of the electoral environment. The Assembly expresses its serious concern that foreign interference operations, through the manipulation of information and voter sentiment, pose a continuing threat in electoral matters to the freedom of voters to form an opinion and to equality of opportunity of candidates and parties.

5. The Assembly, recalling the Reykjavik Principles for Democracy, acknowledges the Committee of Ministers’ ongoing efforts to strengthen democratic resilience and to address democratic backsliding, including its work on countering mis- and disinformation, preventing algorithmic manipulation, and reinforcing electoral integrity. It commends the initiative of the Secretary General to develop a New Democratic Pact to address democratic backsliding, to enhance citizen engagement, and to adapt democratic models to contemporary challenges.

6. In light of the increasing sophistication of multiform foreign interference tactics in the digital sphere, the Assembly welcomes the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225, “the Vilnius Convention”) as an essential tool to promote transparency, accountability and safeguards against AI-driven manipulation and disinformation.

7. In view of the role played by the Council of Europe in ensuring democratic security, the Assembly asks the Committee of Ministers to:

7.1. develop and enhance tools for countering foreign interference that promote a whole-of-society approach, enhance resilience, reinforce public trust, and safeguard institutional integrity;

7.2. consider the feasibility of developing a broad-based, non-binding operational definition of foreign interference to enhance European co-ordination and policy alignment, as well as strengthening clarity on legitimate influence activities.

[3] Draft recommendation adopted by the committee on 5 March 2025.

C. Explanatory memorandum by Ms Zanda Kalniņa-Lukaševica, rapporteur

1. Introduction

1. The Russian Federation's full-scale war of aggression against Ukraine is a watershed moment for European security, with profound implications for democratic security both in Europe and globally. The military aggression is part of a wider systematic attempt to weaken democratic security far beyond Ukraine.

2. The tactics employed by Russia to undermine democracies are well-documented. They include cyberattacks, disinformation campaigns, political subversion, threats to journalists, acts of sabotage, instrumentalised migration, economic coercion, and corruption, all designed to weaken the internal cohesion and resilience of democratic states.[4]

3. These efforts target the very fabric of democracies, seeking to corrode the institutions and principles that have underpinned peace, stability and prosperity in Europe since the end of the Second World War.

4. This playbook of foreign interference is similarly used by other state and non-state actors seeking to challenge systems of liberal democratic governance. These threats have not only grown in scale by exploiting the use of new technologies, but have also diversified, adapting to the unique vulnerabilities of different countries, communities and regions.

5. In response to these evolving threats, member States of the Council of Europe have developed and implemented measures to safeguard their democracies. However, the challenge of foreign interference continues to evolve, requiring constant vigilance, innovation, co-ordination and co-operation at both national and international levels.

6. Democracies must defend themselves against the threat posed by foreign interference as part of an adaptation to an increasingly hostile international environment where the principles of sovereignty, self-determination and democracy are under attack. This need to defend against the threat is reflected by the European public with 81% of respondents to a Eurobarometer survey agreeing that foreign interference in European democratic system is a serious problem that should be addressed, and 74% responding that such interference can affect citizens' voting behaviour.[5] The resilience of democratic institutions is crucial in countering these dangers and ensuring that the values of human rights, democracy and the rule of law prevail. At the same time, responses to foreign interference must be guided by the very principles that they seek to defend.

7. This report will outline the threat of foreign interference to democratic security, and examine approaches taken to counter and to build resilience against foreign interference activities.

2. What is foreign interference?

8. Foreign interference can be described as intentional, covert and manipulative, mostly illegitimate interference by foreign powers, their proxies or private actors with the aim of advancing their political, economic or military goals. It threatens or negatively impacts other States' security, values, democratic procedures, political processes, and their capacity to cope with exceptional situations.

9. This interference targets the foundations of our societies, trying to transform democratic pillars into systemic vulnerabilities, and to turn democracies against themselves.

10. This poses a profound strategic challenge to democratic nations. In an era where the rules-based order is under strain, authoritarian regimes are capitalising on both digital and non-digital arenas with hostile intent. Their primary objective is to internally weaken democracies, eroding the integrity of decision-making processes and undermining public trust in institutions.

11. These malign actions have been accelerated by the systemic and societal challenge of the transformation of the media and information ecosystems and the weakened role of traditional gatekeepers of the public conversation, with the weaponisation of social media for propagating sophisticated information operations posing a potentially existential national security threat to all European democracies.

---

[4] See, for example, United States Senate Committee Print, 115th Congress, Putin's asymmetric assault on democracy in Russian and Europe: Implications for U.S. national security, 2018.
[5] European Commission, Flash Eurobarometer 528, Citizenship and democracy, December 2023.

12. Foreign interference may take different forms, often used in combination, including:

- elite capture;
- covert financing of political life;
- electoral interference;
- disinformation and foreign information manipulation;
- economic coercion;
- transnational control, surveillance and repression of diasporas;
- corruption.[6]

13. Foreign interference is a critical component of the broader universe of hybrid threats, which encompass a blend of military and non-military tactics that are designed to destabilise and exert influence over targeted states.[7]

14. The present report excludes kinetic operations, such as sabotage attacks, assassinations and terrorist actions from its conception of foreign interference.

15. The term "foreign interference" should be distinguished from "foreign influence", as the two concepts, while related, involve different levels of engagement and intention. While there are on occasions grey areas between the two, foreign interference can largely be distinguished by its covert nature and intention to harm the collective interest of the state in question in order to promote the interests of a foreign government.[8]

16. "Foreign influence" typically refers to overt and often legitimate efforts by a foreign government or entity to sway the opinions, policies, or actions of another country. This can take many forms, such as diplomatic engagements, public diplomacy, cultural exchanges, lobbying, and can also include transparent and legal funding of organisations and media organisations.[9] Legitimate, overt foreign influence is a natural part of international relations, with the influencing party generally openly pursuing its interests while engaging with the host country in a manner that respects its sovereignty and legal frameworks.

3. Main foreign interference actors

17. Attribution for foreign interference is complex due to sophisticated methods used to obscure the source of the activity, and further complicated by the use of local proxies or front organisations. The political risk of false attribution and blurred lines between legitimate influence and covert interference add to the challenge presented.

18. Online platforms have been able to track the most frequent sources of foreign interference, with Meta reporting that Russia was the number one source of such operations on their internet infrastructure since 2017, followed by Iran, and China.[10]

19. Studies by parliaments in European parliaments and institutions such as those carried out it France,[11] the Czech Republic,[12] Estonia,[13] Latvia,[14] and the Netherlands,[15] have identified Russia and China as key foreign interference threats to democracies, with tactics that seek to subvert and destabilise societies including long-term disinformation campaigns, information warfare, cyberattacks, and a range of efforts to control narratives abroad, including via influencing university research, and via infiltration in companies.

4. Foreign interference as a threat to democratic security

20. Democratic security is underpinned by the protection and reinforcement of the essential principles, institutions and processes that uphold democratic governance, such as the rule of law, human rights, and free

[6] OECD, Strengthening the transparency and integrity of foreign influence activities in France, 2024, 16.
[7] European Commission, Hybrid Centre of Excellence, The Landscape of Hybrid Threats, A Conceptual Model, 2021.
[8] OECD, Strengthening the transparency and integrity of foreign influence activities in France, 2024, 11.
[9] Government of Canada, Foreign Interference Commission, Influence and interference: distinctions in the context of diplomatic relations and democratic processes, 2024.
[10] Meta, Second Quarter Adversarial Threat Report, August 2024.
[11] French National Assembly, *Rapport fait au nom de la Commission d'enquête relative aux ingérences politiques, économiques et financières de puissances étrangères visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques français*, 2023.
[12] BIS, Security Information Service, Annual report, 2023.
[13] Estonia Foreign Intelligence Service, International Security and Estonia, 2024.
[14] Republic of Latvia, Constitution Protection Services, Annual Report, 2023.
[15] AIVD, Annual Report, 2023.

and fair elections. It includes safeguarding electoral integrity, protecting civil liberties, and promoting an informed and engaged citizenry.[16]

21. Authoritarian regimes have increasingly sought, and with increasing effectiveness, to diminish the integrity of norms and institutions safeguarding fundamental liberties. The tools of foreign interference - such as corruption, disinformation, elite capture, and electoral interference - aim to erode each of the pillars of democratic security.

22. These regimes have actively fuelled and exploited polarisation with Council of Europe member States through these forms of interference. This has included through financial support to extremist groups that amplify divisive, radical and sometimes violent narratives, as well as through funding political movements and politicians in order to sabotage united opposition to hostile actors, while weakening democratic projects and influence.[17]

23. The pattern of destabilisation strategies to erode democratic norms and amplify polarisation seek to weaken trust in the political system, which in turn harms the ability to effectively respond to wider challenges.

24. Free and fair elections are a cornerstone of democratic societies. Independent and transparent electoral processes are necessary for both citizen's trust in our public institutions, and for the competitiveness of the electoral environment. Foreign interference operations are a continuing risk as regards their efforts to manipulate information and voter sentiment, cyberattacks on infrastructure, as well as accessing and leaking sensitive information from governments, political parties and members of parliament.

25. This continually evolving and adapting threat remains difficult to measure, and the cumulative effect of its manifestations on our democracies is not yet fully understood. The rapid advancements and widespread adoption of Artificial Intelligence (AI) have the potential to significantly exacerbate the challenges faced by democracies in confronting foreign interference, and responses will have to adapt in line with these advances.

5. Multiple targets and multiform tactics

26. There are numerous high-profile examples of foreign interference activities threatening democratic security and stability. These activities can be largely grouped into the three main categories of disinformation, cyberattacks and hacking, and financial and political interference.

27. These activities are often employed simultaneously to have a compounding negative effect by systematically targeting the pillars of democratic security. Disinformation undermines the public commons, faith in the credibility of the media, the government and even facts themselves. Cyberattacks compromise sensitive data, disrupting essential services, and bolster disinformation by the selective leaking of materials that feed divisive narratives. Financial and political interference erodes institutional integrity and increases public cynicism about governance.

28. Together, this creates a feedback loop. Cyberattacks provide material for disinformation and leverage over personalities who have had their data compromised, while financial and political interference amplifies distrust created by cyberattacks and disinformation campaigns. The cumulative effect of these can expose systemic vulnerabilities, creating openings for hostile actors to manipulate and destabilise target societies.

5.1. Disinformation

29. Disinformation has been defined by the Council of Europe's Committee of Ministers as verifiably false, inaccurate or misleading information deliberately created and disseminated to cause harm or pursue economic or political gain by deceiving the public.[18]

30. While disinformation is no novelty in the conduct of international relations, the advent of digital technologies has increased its scope to unprecedented levels. Disinformation campaigns involve spreading false or misleading information - typically launched through state-controlled media, social media, or covert

[16] See, for example, Council of Europe, Secretary General, State of democracy, human rights and the rule of law in Europe: A shared responsibility for democratic security in Europe, 2015.
[17] Rekawek, Kacper, Thomas Renard, and Bàrbara Molas, ed(s)., Russia and the Far-Right: Insights from Ten European Countries, International Centre for Counter-Terrorism, 2024.
[18] Council of Europe, Recommendation CM/Rec(2022)12 on electoral communications and media coverage of election campaigns, 6 April 2022.

channels - to shape public opinion, amplify domestic political divisions on sensitive topics, or damage the credibility of specific institutions, processes, or individuals.

31. Disinformation campaigns have become a regular phenomenon, especially during election or referendum campaigns. Irregularities in electoral processes stemming from foreign interference reflect the transformative impact of digital threats to elections. In December 2024, the Romanian Constitutional Court annulled the result of presidential election first round and ordered that the elections should be reorganised from the start by the Government on a future date after the Court found that there had been a breach of the "essential principles of free democratic elections".[19] The Court's decision came after intelligence documents were declassified that suggested that one of the candidates benefitted from a mass influence operation – conducted from abroad – that manipulated the votes and distorted equal opportunities of electoral competitors through the use of digital technology and artificial intelligence.

32. In coming to this decision, the Constitutional Court found that states must be resilient in the face of challenges and risks generated by organised disinformation campaigns that affect the integrity of electoral processes, and reasoned that the freedom of voters to form an opinion includes the right to have access to accurate information about candidates and the electoral process as well as a protection against unjustified influence on their voting behaviour through unlawful and disproportionate acts or facts. It stated that electoral online publicity must always be identified as such and be transparent, both with regard to the identity of the sponsor, as well as with regard to the technical means of dissemination.[20]

33. State-funded media outlets are a key vector for disinformation, with prominent examples being Russia's Sputnik and RT, as well as China's Global Television Network. These outlets are under the permanent direct or indirect control of state authorities and are instrumental in the systematic propagation of disinformation.

34. Internal foreign policy concept documents from hostile actors have made clear that this disinformation is a strategic action, such as the Russian Ministry of Foreign Affairs calling for an "offensive information campaign" across the "military-political, economic and trade and informational psychological spheres".[21]

35. In 2017, a report commissioned by the Council of Europe called the increased use of disinformation one of the elements of wider information disorder.[22] Even when specific disinformation campaigns are successfully revealed and debunked, the cumulative effect of persistent false information has been to erode trust in the information environment, with research from the OECD showing that on average only 39% of people have high or moderately high trust in news media, while 44% report low to no trust in the media.[23]

36. Disinformation networks have proliferated following the full-scale war of aggression of the Russian Federation against Ukraine to scale up pro-Kremlin narratives on social media platforms, both in Europe and globally.

37. Russian-based influence operations include tactics such as used in "DoppelGänger", where hostile actors developed websites that impersonated established news organisations or government websites in Council of Europe member States. Disinformation stories were then placed on these spoof sites to give an appearance of authenticity and disseminated on social media sites through a network of false accounts.[24]

38. Between 24 February 2022 and October 2023, monitoring conducted across six countries (Germany, Italy, Poland, Czech Republic, Slovakia and Hungary), found the dissemination of over 13 000 disinformation messages clustered around key pro-Russian narratives.[25]

39. The rapid amplification of disinformation narratives by hostile states is facilitated by bots and artificial intelligence in order to increase external pressure on the policymakers by local populations and spread false narratives about the illegal actions being undertaken by Russia in Ukraine.

40. Research by the French agency VIGINUM showed that between September and December 2023, a network of 200 disinformation portals was detected that converted disinformation content into target audience languages.[26]

[19] Constitutional Court of Romania, Decision no. 32, 6 December 2024.
[20] Constitutional Court of Romania, Decision no. 32, 6 December 2024.
[21] Resolution, Board of the Ministry of Foreign Affairs of the Russian Federation, 11 April 2023.
[22] Council of Europe, Information disorder: Towards an interdisciplinary framework for research and policy making, 2017.
[23] OECD, Survey on drivers of trust in public institutions- 2024 Results, 10 July 2024.
[24] EU Disinfo Lab, Doppelganger – Media Clones Serving Russian Propaganda, 27 September 2022.
[25] VoxCheck, Investigation into Russian Falsehoods in Europe, 16 November 2023.
[26] VIGINUM, Technical Report, February 2024.

41. Chinese-affiliated disinformation or propaganda has, according to data from Microsoft, been deployed at a “scale unmatched by other malign influence actors”, through the use of thousands of accounts across a range of internet platforms spreading memes, videos, and articles in multiple languages.[27]

42. Disinformation operations have also sought to exploit sensitive issues in target countries to exacerbate social divides. Referred to as “parasitic” operations, these operations opportunistically amplify existing inflammatory content or domestic misinformation via bots to exacerbate tensions on certain issues and promote extreme views. The dynamic between foreign disinformation and domestic misinformation can have a catalysing effect on domestic groups. This has been seen during the Covid-19 pandemic to exacerbate vaccine hesitancy and pandemic conspiracy theories,[28] and in accelerating domestic tension related to migration or electoral security.

43. These disinformation campaigns have on occasion been carried out in concert with further hybrid actions. This has particularly been the case with regards to the weaponisation of migration flows with the intent of destabilising European democracies. Hybrid foreign interference strategies have included the transportation of migrants and asylum seekers by Belarus and by Russia to the borders of Poland, Lithuania, Latvia, and Finland. Supporting disinformation campaigns then exploit migrants, minorities, and diasporas as conduits for malign disinformation campaigns. The aim is to amplify and exploit existing negative perceptions about migration, consequently fostering heightened tensions within European societies.

5.2. Cyberattacks and hacking

44. As digital technologies have become pervasive in all aspects of life – including administration, defence, critical infrastructure and the economy, there has been growing convergence between foreign interference operations driven by disinformation campaigns and State or State-sponsored cyberattacks as a vector for interference.

45. Cyberattacks and hacking attempts directed at state institutions disrupt access to government websites, obstruct governmental bodies, and compromise officials’ email accounts. As well as posing a threat to the provision of essential services and public safety, such activity exposes government networks to hostile actors, and government officials’ communications and influence democratic processes. In 2024 alone, hostile cyber operations in Europe were publicly attributed to pro-Kremlin hackers, including in the Czech Republic, Germany, Greece, Poland and Switzerland.[29]

46. The threats to elections from foreign interference have included the hacking of emails of candidates, such as in the American presidential election in 2016,[30] and the French presidential elections of 2017, and attempts to affect the electoral infrastructure itself, such as cyberattacks in Ukraine in 2014, North Macedonia in 2019, and the Republic of Moldova in 2019.[31]

47. In December 2023, the United Kingdom exposed attempted Russian cyber interference in political processes. These operations targeted parliamentarians through spear-phishing campaigns, hacking and leaking UK-US trade documents, and interference against UK think tanks on defending democracy against disinformation.[32]

5.3. Financial and political interference

48. Elite capture and corruption are insidious forms of foreign interference that can undermine democratic security. The co-opting of key political, business or media elites to advance the interests of a foreign state come at the expense of national sovereignty and democratic norms. It diminishes the effectiveness and legitimacy of institutions and erodes the rule of law.

49. Alleged attempts by foreign countries such as Qatar to influence Members, former Members, and staff of the European Parliament through acts of corruption would represent a serious interference in European

---

[27] Microsoft, Digital Defense Report, October 2023.
[28] EEAS, Special Report, Short Assessment of Narrative and Disinformation around the COVID-19 Pandemic, April 2021.
[29] See, for example, GMF, Alliance for Securing Democracy, Authoritarian Interference Tracker.
[30] U.S. Department of Justice, Special Counsel Robert S. Mueller, Report on the investigation into Russian interference in the 2016 Presidential election, 2019.
[31] Hybrid Centre of Excellence, Countering hybrid threats to elections, 2024.
[32] United Kingdom Foreign, Commonwealth & Development Office, Press release, 7 December 2023.

democratic processes.[33] The European Parliament also noted in a 2024 resolution that credible allegations have been made that Members of the European Parliament were paid to disseminate Russian propaganda.[34]

50. Further concerns about the funding of political parties in democratic countries by Russia in attempts to interfere in domestic processes have seen the European Parliament call for a comprehensive investigation into potential foreign interference support to secessionist movements, such as in Catalonia after it was alleged that Russian-affiliated envoys met with Catalan independence leaders in 2017 to offer massive financial aid in exchange for favourable cryptocurrency legislation.[35]

51. These concerns have also led to calls for greater transparency into funding for political parties, with an investigation showing that populist, far-right and far-left political parties received a quarter of all private funding to political parties in the European Union between 2019-2022,[36] while intelligence cables stated that Russian provided 300 million USD to influence politicians and officials across 24 countries between 2014-2022.[37]

52. In March 2024, the Czech Republic sanctioned the Prague-based news site Voice of Europe after allegations that it had paid politicians in several European countries to spread anti-Ukraine sentiment and influence the June European Parliament elections as part of a Russian influence operation.[38]

53. Financial foreign interference has also targeted voters in advance of elections. Moldovan authorities consistently raised alarms about attempts of the Russian Federation to interfere in the domestic politics and electoral processes of the Republic of Moldova in 2024, with a large influx of Russian money into the Republic of Moldova reported with the aim of buying votes and subverting the democratic process.[39]

54. The General Police Inspectorate of the Republic of Moldova documented cases of bribery that involved 130 000 citizens and over 15 million USD in illicit transfers from Russia in September 2024 alone.[40] The scale of vote-buying schemes was estimated to be higher overall, with funds dispersed through a range of schemes such as “social” allowances for pensioners, and salary “bonuses” for employees of local government structures.[41]

6. The response

55. The Council of Europe, its member States and international organisations have developed a range of tools to prevent, detect, counter and sanction the multifaceted threat posed by foreign interference.

6.1. Updating security concepts

56. The Russian Federation’s large-scale aggression against Ukraine, and its hybrid character, have highlighted the urgency for democracies to update their national security concepts.

57. Member States have consequently sought to amend strategies that incorporate actions to confront the risk from accelerated foreign interference operations. Germany, for instance, has adopted its first ever national security strategy.[42] Based on a broad concept of security, this document aims to provide comprehensive answers to the diverse security challenges of our time. This goes far beyond traditional defence political issues and includes matters ranging from development of co-operation to the defence against cyber risks.

58. Entities have been created to adapt to the activities of hostile actors, such as the establishment in France in 2021 of the national agency VIGINUM, the service for vigilance and protection against foreign digital interference. Its role is to detect online threats that seek to undermine France’s fundamental interests.

---

[33] European Parliament resolution of 1 June 2023 on foreign interference in all democratic processes in the European Union, including disinformation (2022/2075(INI)).
[34] European Parliament resolution of 25 April 2024 on new allegations of Russian interference in the European Parliament, in the upcoming EU elections and the impact on the European Union (2024/2696(RSP); & David E. Alandete “Russian Interference in the Catalan Independence Crisis (2014-2022)”.
[35] European Parliament resolution of 1 June 2023 on foreign interference in all democratic processes in the European Union, including disinformation (2022/2075(INI)).
[36] Follow the Money, Transparency Gap: The funding of political parties in the EU, 2024.
[37] BBC, Russia covertly spent $300m to meddle abroad – US, 14 September 2022.
[38] Ministry of Foreign Affairs of the Czech Republic, Press release, 28 March 2024.
[39] Parliamentary Assembly, Press release, 5 July 2024.
[40] IPN, $15 million transferred from Russia for corrupting voters in Moldova, 3 October 2024.
[41] Atlantic Council, What to know about Russian malign influence in Moldova’s upcoming election, 18 October 2024.
[42] National Security Strategy | BMVg.de.

59. In 2023, France and Slovenia, in partnership with Montenegro, founded the Western Balkans Cyber Capacity Centre in order to build long-term cyber capacity to confront cyberattacks and online disinformation by foreign actors seeking to provoke instability in the region.[43]

60. One month into the Russian Federation's war of aggression against Ukraine, the Council of the European Union approved the Strategic Compass to set out a common strategic vision for EU security and defence policy over the next 5-10 years.[44] Tellingly, its full title is "For a European Union that protects its citizens, values and interests and contributes to international peace and security". Assessing the shared strategic environment, the document describes the complex security threats confronting the EU, including:

- hybrid threats growing in frequency and impact;
- soft power being weaponised, with vaccines, data and technology being used as instruments of political competition;
- increasing attempts of economic and energy coercion.

61. Amongst the instruments foreseen by the Strategic Compass is a European Union Hybrid Toolbox to detect and respond to a broad range of hybrid threats, which includes a dedicated actions to address foreign information manipulation and interference. The European Union already has a range of options for the European Union Hybrid Toolbox implementation, such as the Cyber Diplomacy Toolbox,[45] and the added value of the Hybrid Toolbox is to enable a fast, coherent and co-ordinated response, gathering a combination of civilian and military instruments.[46]. The Council of the European Union approved the guiding framework for the practical establishment of European Union Hybrid Rapid Response Teams in May 2024 that can be deployed upon request to prepare against and counter hybrid threats.[47]

62. In June 2022 in Madrid, NATO adopted a New Strategic Concept, which recalled that "strategic competitors test our resilience and seek to exploit the openness, interconnectedness and digitalisation of our nations […] These actors are also at the forefront of a deliberate effort to undermine multilateral norms and institutions and promote authoritarian models of governance." [48] It called for efforts to develop resilience against and counter foreign interference and hybrid threats being levelled against NATO Allies and countries aspiring to become members of the Alliance.

6.2. Developing societal resilience

63. With hybrid threats set to continue to affect the security landscape, developing societal resilience against foreign interference needs a comprehensive, whole-of-society approach. Efforts to influence elections from abroad have been shown to be more likely to take place through voter manipulation over the long term rather than through direct attacks on the election system. Protective measures therefore require a strong focus on the overall resilience of the population to foreign influence.[49]

64. Developing societal resilience against foreign interference is imperative for safeguarding democratic institutions and ensuring the integrity of electoral processes. This involves multifaceted strategies encompassing education, media literacy, and the cultivation of critical thinking skills among citizens to discern and counter disinformation. Strengthening public awareness about the tactics used by foreign actors in spreading false narratives, especially through social media platforms, is crucial.

65. Finland has incorporated media literacy into its national curriculum from an early age, equipping students with essential skills to navigate today's complex information landscape. Finnish schools teach children how to evaluate the credibility of various information sources, identify biased or misleading content, and understand the motivations behind disinformation campaigns.[50] Estonia and Latvia have sought to enhance media literacy by respectively working to strengthen the resilience of their Russian-speaking populations against information manipulation, offering alternatives to Russian media and engaging with its Russian-speaking minority,[51] and supporting and training independent journalism at institutes such as the Riga-based Baltic Centre for Media Excellence.

---

[43] Statement, Cyber security – Signing of the treaty on the Western Balkans Cyber Capacity Centre, 16 October 2024.
[44] A Strategic Compass for a stronger EU security and defence in the next decade - Consilium (europa.eu).
[45] The EU Cyber Diplomacy Toolbox (cyber-diplomacy-toolbox.com).
[46] European Parliament, NATO supports Hybrid Toolbox - Sundsvall Idag.
[47] Council of the EU, Press release, Hybrid threats, 21 May 2024.
[48] NATO, Press release, NATO leaders approve new Strategic Concept, 29 June 2022.
[49] https://www.hybridcoe.fi/wp-content/uploads/2023/09/20230912-Hybrid-CoE-Research-Report-10-PEI-WEB.pdf
[50] OECD, Facts not fakes: Tackling disinformation, strengthening information integrity, 2024, 73.
[51] IFES, Building Resilience Against Election Influence Operations: Preparing for the European Elections in 2024 and Beyond, 2024.

66. Additionally, fostering a diverse and independent media landscape that upholds journalistic integrity and fact-checking practices can mitigate the spread of disinformation. Collaboration between governments, civil society organisations, and tech platforms is pivotal in implementing effective strategies to identify, counter, and raise awareness about foreign interference. Empowering communities, including minorities and vulnerable groups often targeted by disinformation campaigns, through inclusive and informative initiatives will contribute significantly to fortifying societal resilience against external manipulation and preserving the democratic fabric of nations.

67. The European Commission Joint Research Centre with the Hybrid Centre of Excellence has proposed a methodology for a comprehensive resilience mechanism, which seeks to provide a system for the detection of early signals, help analysis of hybrid threats, and identify potential response trajectories.[52]

68. The Nordic and Baltic States apply the concept of "total defence", on the basis of which the whole society - the armed forces and civil society – is involved in preventing, deterring and countering an attack. In 2018, the Sweden's Civil Contingencies Agency (MSB) sent a booklet to all households with guidelines on how citizens should protect themselves from false information and cyberattacks as well as many other threats.[53]

6.3. Countering disinformation

69. Enhancing societal resilience to combat foreign interference is part of a wider toolkit for effective and successful counter-disinformation capability. While efforts to combat disinformation need to protect freedom of expression and access to information, States have enhanced efforts to counter disinformation by disrupting foreign interference actors, such as by pre-bunking and via content correction.

70. As part of disruption methods, state authorities have identified and dismantled bot farms spreading disinformation, such as Russian-based disinformation networks operating in the United States of America being shut down in July 2024,[54] and the cyber police in Ukraine suspending the activities of 13 bot farms with more than 1.5 million fake social media accounts that were registered for spreading disinformation and propaganda.[55] Online platforms have also taking measures against coordinated efforts to manipulate public debated for strategic goals where fake accounts are central to the operation, with Meta identifying 39 covert influence operations from Russia between 2017 and 2024, with the next most frequent sources of covert influence operations emanating from Iran and China.[56]

71. To address the risks of artificial intelligence technology generating false information or exacerbating manipulative content curation to undermine information integrity, the Council of Europe's Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225, "the Vilnius Convention") provides that signatories shall maintain measures that ensure artificial intelligence systems are not used to undermine the integrity, independence and effectiveness of democratic institutions and processes, and that protect democratic processes including the ability to freely form opinions.[57]

72. Governments have increasingly used strategic communications to 'pre-bunk' disinformation by declassifying intelligence. The United States notably employed this approach to expose Russian decision-making in the lead-up to Russia's February 2022 invasion of Ukraine, and to meaningfully undercut Russian narratives.

73. Several European countries have improved intergovernmental co-ordination. Germany established an inter-ministerial taskforce led by the Federal Ministry of the Interior and Community to foster close cooperation on responses to hybrid threats, especially disinformation. This taskforce coordinates all activities against the deliberate spread of false and misleading information in the context of the war against Ukraine, including strengthening proactive and transparent communication and enhancing societal resilience against threats in the information space.[58]

[52] European Commission, Hybrid Threats: A Comprehensive Resilience Ecosystem, 2023.
[53] Countering information influence activities : A handbook for communicators (msb.se).
[54] US Department of Justice, Press release, 9 July 2024.
[55] Cyber Police of Ukraine, Press release, 20 December 2022.
[56] See, for example, Meta, Second Quarter Adversarial Threat Report, August 2024.
[57] See, Explanatory Report to the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, 5 October 2024.
[58] G7, Rapid Response Mechanism Annual Report, 2022.

74. Efforts to counter disinformation via content correction have seen a growing network of independent, non-partisan, fact-checking organisations, often working in collaboration with media outlets and digital platforms to identify and correct false information. These fact-checkers often publish corrected information prominently and work to ensure that misinformation is not only debunked but also replaced with factual narratives.

75. The Council of Europe's Steering Committee on Media and Information Society adopted in December 2023 a Guidance Note on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner which stressed the centrality of fact-checking as a key institution of public debate and called for the independence of fact-checking organisations vis-à-vis states.[59]

76. Globally, the United Nations launched the United Nations Global Principles for Information Integrity in 2024, which aim to combat misinformation, disinformation and hate speech while upholding human rights, including the freedom of expression.[60] The principles are addressed to a range of stakeholders, and are centred around societal trust and resilience, public empowerment, independent, free and pluralistic media, as well as transparency.

77. At the European Union level, a comprehensive approach has been taken, which includes the Digital Services Act which obliges digital platforms to take more responsibility for the content that appears on their services. The strictest obligations of the Act are applicable to very large online platforms and search engines, defined as online platforms and intermediaries that have more than 45 million users per month in the EU. Such platforms have to identify and address any systemic risks their platforms pose, such as those related to fundamental rights, public security, and elections.

78. Specialised task forces have been established, such as the East StratCom Task Force, to expose and debunk disinformation narratives, while projects to improve media literacy have supplemented these efforts in order to enhance long-term resilience to disinformation.

79. At the national level, the establishment of agencies and institutions to combat the threat has accelerated. The Swedish Psychological Defence Agency, established in 2022, plays a crucial role in safeguarding Sweden's information environment and ensuring its societal resilience against foreign interference. The Agency has both an operational role and a mandate to strengthen societal resilience against foreign interference. The Psychological Defence Agency identifies, analyses and provides support in countering malign information influence and other misleading information that is directed at Sweden or Swedish interests by antagonistic foreign powers. This can concern disinformation aimed at weakening Sweden's resilience and the willingness of the population to defend itself, or unduly influencing people's perceptions, behaviours and decision-making.

80. Several European countries have launched special investigative committees devoted to countering Russian influence. For example, in May 2024, the Commission for Investigating Russian and Belarusian Influence was established in Poland by order of the Prime Minister. The Commission is hosted by the Minister of Justice and will investigate cases of Russia and Belarus exerting influence on Poland's politics since 2004.

81. Increased efforts to partner across government, online platforms and law enforcement have been noted in recent years. The 2022 Code of Practice on Disinformation, elaborated by the European Union with major online platforms, emerging and specialised platforms, players in the advertising industry, fact-checkers, research and civil society organisations, seeks to expand fact-checking, cut financial incentives for spreading disinformation, and cover manipulative behaviours such as fake accounts, bots or malicious deep fakes.

82. In efforts to disrupt the Russian disinformation ecosystem, the European Union has suspended the broadcasting activities and licences of several Kremlin-backed disinformation outlets. These outlets have been used by the Russian government as instruments to manipulate information and promote disinformation about the military aggression against Ukraine, including propaganda aimed at destabilising the countries neighbouring Russia, the EU and its member states.

83. Observing that Sputnik and Russia Today were under the permanent direct or indirect control of the authorities of the Russian Federation and essential and instrumental in bringing forward and supporting the military aggression against Ukraine, the Council of the European Union explained its decision on the grounds

[59] Council of Europe, Guidance Note on countering the spread of online mis-and disinformation through fact-checking and platform design solutions in a human rights compliant manner, 2024.
[60] United Nations, Global Principles for information integrity: Recommendations for multi-stakeholder action, June 2024.

that "the Russian Federation has engaged in a systematic, international campaign of disinformation, information manipulation and distortion of fact in order to enhance its strategy of destabilisation of its neighbouring countries, the EU and its member States. (…) In order to justify and support its military aggression of Ukraine, the Russian Federation has engaged in continuous and concerted disinformation and information manipulation actions targeted at the EU and neighbouring civil society members, gravely distorting and manipulating facts".[61]

84. Individuals involved in the dissemination of propaganda and disinformation have also been sanctioned. For example, the Editor-in-chief of RT, Margarita Simonyan was sanctioned by the European Union as a central figure of the Russian Government propaganda responsible for actions and policies which undermine the territorial integrity, sovereignty and independence of Ukraine.

85. The effect of the suspension of the broadcasting activities in the first six months since their initial announcement in 2022 saw visits via search engines to the sanctioned outlets reduced by 100%, visits via social media by 70%, and web traffic from the EU by 74%.[62] Court appeals against the ban by outlets of RT were rejected, as the suspension was a proportionate measure against active support to a wider destabilisation policy capable of constituting a significant and direct threat to public order and security.[63]

6.4. Ensuring transparency of foreign influence

86. The effective management of conflicts of interest, lobbying, and political financing are particularly important for confronting vulnerabilities to the risks of foreign interference and its destabilising effect on democracy.[64] Concerns about foreign influence on domestic affairs and public opinion have led a number of countries around the world to adopt legislation aimed at ensuring greater transparency as a first step to preventing threats.

87. Regarding the transparency and regulation of donations to political parties and electoral campaigns, the Council of Europe Committee of Ministers called in 2003 for member States to specifically limit, prohibit or otherwise regulate donations from foreign donors.[65]

88. The Parliamentary Assembly has condemned all attempts to interfere improperly or illicitly in democratic decision-making processes in other states through financial contributions to political parties and electoral campaigns. It called on member States to review their regulations governing financial contributions to political parties and electoral campaigns from foreign sources to mitigate the risk of inappropriate or illicit foreign financial interference.[66]

89. The Assembly has also called on national governments to enhance measures for preventing corruption and called on national governments to adopt and update codes of ethics for all holders of public office.[67]

90. In 2023, the Council of Europe's Group of States against Corruption (GRECO) launched a follow-up procedure to the theme of transparency of party funding to improve the legal framework in this area and to ensure that all its member states now have related legislation. Recommendations of GRECO from its 4th evaluation round dealt with the prevention of corruption in respect of members of parliament, judges and prosecutors. They include ensuring codes of conduct for parliamentarians to ensure enforceable, publicly shared standards for professional conduct, improving transparency, and reducing the vulnerability of parliamentarians to undue influence.

91. On 22 March 2022, the EU Council reached political agreement on the recast of the regulation on the statute and funding of European political parties and European political foundations. This revision aims to enhance the transparency of European political parties and bolster the framework for their funding, in particular to counter the risks of foreign interference and manipulation.[68]

---

[61] EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU - Consilium (europa.eu).
[62] Institute for Strategic Dialogue, Effectiveness of the Sanctions on Russian State-Affiliated Media in the EU, October 2022.
[63] See, for example, CJEU, Judgment of the General Court, *RT France v Council,* (T-125/22), 27 July 2022.
[64] OECD, Anti-corruption and Integrity Outlook, 2024
[65] Committee of Ministers, Recommendation Rec(2003)4 on common rules against corruption in the funding of political parties and electoral campaigns, 8 April 2003.
[66] Resolution 15302 (2021), Transparency and regulation of donations to political parties and electoral campaigns from foreign donors, 31 May 2021.
[67] Resolution 2406 (2021), Fighting corruption – General principles of political responsibility, 26 November 2021.
[68] Council of the EU takes steps towards more transparent funding of European political parties - Consilium (europa.eu).

92. States have taken a range of further measures to improve transparency on the links between natural or legal persons operating in the public arena and carrying out influence activities on behalf of foreign state interests. These can strengthen the integrity of foreign influence activities, allow decision-makers and citizens to know whose interests are being defended, and demarcate more clearly between legitimate influence activities, and illegitimate interference attempts.[69]

93. An early example of these efforts was the Foreign Agents Registration Act (FARA), which was introduced in the United States in 1938 to counter Nazi propaganda. With significant changes, this law is still in force, with the purpose to identify foreign influence in the United States and address threats to national security. The act requires "agents of foreign principals in a political or quasi-political capacity to make periodic public disclosure" of that relationship. Activities taken as a result of it must also be disclosed.[70]

94. In March 2023, Canada announced the opening of consultations to lay the groundwork for a foreign agent registry, amidst media reports detailing alleged Chinese meddling in the country's past two elections.[71]

95. Australia had already done so in 2018, after intelligence reports described extensive influence operations by China at all levels of government for the previous decade, including millions of dollars in political donations and concerns about the Chinese Communist Party monitoring and manipulating Chinese nationals in Australia.[72]

96. In 2023, the UK government presented the Foreign Influence Registration Scheme (FIRS), which aimed to strengthen the resilience of the UK political system against covert foreign influence and provides greater assurance around the activities of certain foreign powers or entities that are a national security risk. FIRS requires the registration of arrangements to carry out political influence activities in the UK at the direction of a foreign power. The enhanced tier of FIRS gives the Secretary of State the power to require registration of a broader range of activities for specified countries, parts of countries or foreign government-controlled entities where this is necessary to protect the safety of interests of the UK.[73]

97. The European Commission, as part of its Defence of Democracy package proposed a new directive on the transparency of interest representation on behalf of third countries in December 2023,[74] and held public consultations on a proposal which sought to harmonise requirement in relation to economic activities of interest representation carried out on behalf of third country entities.[75] This proposal would enhance the already existing Transparency Register.[76]

98. Human rights standards must guide the elaboration and implementation of transparency laws related to foreign influence in order to protect fundamental freedoms including the freedom of expression, freedom of association and privacy. The Council of Europe Venice Commission has accepted that the foreign funding of associations "may give rise to some legitimate concerns",[77] but restrictive measures on funding must be strictly necessary and proportionate to the legitimate aim. Freedom of association is a fundamental human right that is crucial to the functioning of a democracy, and associations such as interest groups, trade unions, and political parties are all crucial elements of a democratic state.

99. The full respect of international standards in the elaboration of transparency instruments is key to avoiding undue restrictions on civil society and adverse effects on open, informed public debate, pluralism and democracy. It is of the utmost importance that these laws are drafted based on an inclusive consultation process, include precise definitions and foresee clear obligations and proportionate sanctions. The overall democratic, human rights and rule of law environment and discourse are also key elements to be taken into consideration when assessing these pieces of legislation.

---

[69] OECD, Strengthening the transparency and integrity of foreign influence activities in France, 2024.
[70] Foreign Agents Registration Act | Foreign Agents Registration Act (justice.gov); Foreign Agents Registration Act (FARA): A Legal Overview (fas.org).
[71] Canada starts setting up foreign agent registry amid reports of Chinese election meddling | Reuters.
[72] What's in Australia's New Laws on Foreign Interference in Domestic Politics - Lawfare (lawfareblog.com).
[73] Foreign Influence Registration Scheme factsheet - GOV.UK (www.gov.uk).
[74] European Commission, Proposal for a Directive of the European Parliament and of the Council establishing harmonised requirements in the internal market on transparency of interest representation carried out on behalf of third countries and amending Directive (EU) 2019/1937.
[75] EU 'foreign agents' law spooks NGOs – POLITICO.
[76] Transparency register (europa.eu).
[77] CDL-AD(2014)046, Joint Guidelines on Freedom of Association, para 221.

100. The Assembly has recalled that non-governmental organisations are a key component of an open and democratic society and make an essential contribution to the development and realisation of democracy, the rule of law and human rights. It has expressed its concern that member States have used legislation imposing excessive reporting and public disclosure obligations on NGOs receiving funding from abroad, in order to stigmatise these organisations, and therefore called on member States to comply with international legal standards with regards to the rights to freedom of assembly, association and expression.[78]

101. The risk of abuse of such legislation has been shown by Russia's "foreign agent" law, enacted in 2012 and later expanded. It has been used as a tool of repression to curtail freedom of expression, persecute opposition figures, and clamp down on human rights organisations. 200 organisations were registered as foreign agents between 2012 and February 2021. As of February 2022, there were still 73 organisations on the list, the remainder having either closed down or been delisted. The overly broad and discriminatory scope of the legal regime could not be found to be necessary in a democratic society.[79]

7. International co-operation

102. Foreign interference often transcends national borders, with state and no-state actors leveraging digital platforms, financial networks and transnational alliances to disrupt democratic processes. Collaboration is needed at the international level in order to enhance capabilities to detect, deter and respond to foreign interference consistently, robustly and in a way that is aligned with international standards. A number of initiatives between like-minded states to respond to the threat have been launched that provide a platform for this collaboration.

7.1. The European Centre of Excellence for Countering Hybrid Threats in Helsinki[80]

103. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) is an autonomous, network-based international organisation promoting a whole-of-government and whole-of-society approach to countering hybrid threats.

104. Participation in the Centre's activities is open to all European Union and NATO countries, and the number of Participating States had grown to include 36 States by November 2024. Its mission is to strengthen its Participating States' and organisations' security by providing expertise and training for countering hybrid threats. The Centre's vision is a world in which our open, democratic societies operate free of malign outside interference.

105. The Centre's key task is to build its Participating States' capabilities to prevent and counter hybrid threats. This is achieved by sharing best practice, providing recommendations, as well as testing new ideas and approaches. The Centre also builds the operational capacities of the Participating States by training practitioners and organising hands-on exercises.

106. The Hybrid CoE develops new strategic concepts and helps to implement them through its cross-governmental, cross-sectoral networks, which consist of over 1 500 practitioners and experts working variously in the Participating States, the European Union and NATO, the private sector, and academia.

7.2. NATO Centres of Excellence

107. There are two NATO-accredited Centres of Excellence that are of relevance in combatting foreign interference. These centres are supported by groups of international experts from military, government, academia and interest.

108. The NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn was established following the 2007 cyberattack against Estonia. It is a knowledge hub which offers a unique interdisciplinary approach to the most relevant issues in cyber defence. It conducts research, trainings, and exercises in four core areas: technology, strategy, operations and law.

[78] Resolution 2362, Restrictions on NGO activities in Council of Europe member States, 27 January 2021.
[79] European Court of Human Rights, *Ecodefence and others v. Russia*, nos. 9988/13 and 60 others, 14.06.2022; Venice Commission, Opinion on the Compatibility with international human rights standards of a series of Bills introduced to the Russian State Duma between 10 and 23 November 2020, to amend laws affecting "foreign agents", 2-3 July 2021.
[80] About us - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats.

109. The NATO Strategic Communications Centre of Excellence (Stratcom COE) in Riga was established in 2014. It is a research and information hub on the subject of strategic communications, encompassing countering disinformation, digital security, and the methodologies of hostile actors.

7.3. The G7

110. In the Capri Communiqué of April 2024, G7 Foreign Ministers committed to protecting the information environment and democratic values against any attempt at foreign manipulation. This included strengthening public resilience to and awareness about foreign information manipulation.[81]

111. A platform for addressing these threats, the G7 Rapid Response Mechanism (RRM) was established in the “Charlevoix Commitment on Defending Democracy from Foreign Threats" issued by the leaders of the G7 - United States, Canada, Japan, United Kingdom, France, Germany, and Italy - in June 2018, during their summit in Charlevoix, Quebec. The mandate of this mechanism is to strengthen the co-ordination of G7 member countries "to identify and respond to diverse and evolving threats to our democracies, including through sharing information and analysis, and identifying opportunities for co-ordinated response".[82] It publishes an annual report identifying challenges and trends in the area of disinformation affecting the G7.

8. Conclusions

112. Council of Europe member States are confronted with a deteriorating security environment in which hybrid threats and foreign interference are increasingly significant. These challenges extend beyond traditional security concerns and have evolved to exploit societal vulnerabilities, undermining the values that are fundamental to our way of life such as democracy, the rule of law, and human rights. As a result, foreign interference represents a direct threat not only to the democratic security of individual member States, but also to the preservation of peace and stability.

113. Countering malicious foreign interference is an inherently complex task for several reasons. First, foreign interference is an evolving threat which manifests in different ways and changes with technological advancements. The diverse range of tactics make it a challenge to recognise and define such interference in a consistent manner.

114. Additionally, accurately identifying and attributing interference is difficult. Covert tactics and the use of proxy actors make it a challenge to discern whether activities are locally driven or orchestrated from hostile foreign actors. Domestic actors participate in the spread of disinformation narratives either organically or in collaboration with foreign entities, further blurring the lines of responsibility. Measuring the true impact of such interference is a delicate task, as the effects can be subtle, gradual, and difficult to quantify, yet they erode public trust and social cohesion over time.

115. Given these intricacies, effective responses must be multifaceted, drawing on a range of measures to bolster resilience and safeguard democratic values. Facilitating a whole-of-society response by building societal resilience is essential, beginning with widespread digital education and awareness campaigns that help citizens identify and counter disinformation. Strengthening protections for fact-checkers, civil society, and investigative journalists, who are vital in exposing disinformation and foreign influence, is also critical.

116. In many states, there is no legislation or legal definition of hybrid threats or disinformation, which means that there are no specific laws or regulations in place to combat them effectively. As a result, there is a significant gap between the nature of the threat and the ability of governments to effectively counter it through legal means.[83]

117. The European University Institute's Media Pluralism Monitor 2022 found that 15 of 32 countries analysed (including the EU's 27 Member States) had some form of regulatory framework within which to fight disinformation. However, only the frameworks in Finland, Germany and Lithuania were deemed efficient.[84]

118. In developing policy responses to foreign interference, it is vital that all measures taken align with established human rights standards. While the threat posed by foreign interference is real and pressing, it is

[81] G7, Foreign Ministers’ Meeting Communiqué, Capri, 19 April, 2024.
[82] G7, Rapid Response Mechanism, Annual Report, 2021
[83] Hybrid CoE, Research Report 10, Preventing election interference: Selected best practices and recommendations, 2023.
[84] EUI, Media Pluralism Monitor, 2022.

crucial that responses do not undermine the very principles they aim to protect. Human rights, the rule of law, and democratic freedoms must remain at the forefront of any strategy to counteract interference. This approach not only reinforces the legitimacy of countermeasures, but also distinguishes democratic responses from the covert, often repressive tactics used by hostile actors.

119. Measures that disregard human rights risk creating a counterproductive effect, as they may erode public trust and fuel perceptions of government overreach. For instance, while digital monitoring or restrictions on information channels might seem effective in the short term, such actions must be carefully calibrated to avoid infringing on freedom of expression, privacy, and the right to access information. Transparent procedures, adherence to due process, and respect for individual rights must guide any enforcement actions taken against disinformation or destabilisation efforts.

120. By ensuring these measures are guided by human rights standards, Council of Europe member States can foster a balanced, effective approach that secures both national security and the democratic rights of their citizens.