**48th SESSION**

Report
CG(2025)48-10
26 March 2025

# Foreign interference in electoral processes at local and regional levels

Committee on the Monitoring of the implementation of the European Charter of Local Self-Government and on the respect of Human Rights and the Rule of Law at local and regional levels (Monitoring Committee)

Rapporteur:[1] Stewart DICKSON, United Kingdom (R, ILDG)



*Summary*

In the 2023 Reykjavik Declaration, Council of Europe member States reaffirmed their commitment to hold elections and referenda in accordance with international standards and take all appropriate measures against any interference in electoral systems and processes. In this regard, the Congress has long held the conviction that local and regional elections must be decided by voters of the community in which they reside. However, as a result of their increasing significance in the electoral landscape, local and regional elections have become increasingly vulnerable to foreign interference with a view to distorting the will of voters and influencing the outcome of elections, as the Congress has observed in some member States. While the impact and success of such acts remain difficult to assess, the multiplication of cases can further erode voters' trust in democratic processes.

At the same time, despite existing international standards, the lack of specific protection for local elections leaves them vulnerable. While corruption at the local level is well documented, foreign interference remains under-researched and difficult to detect and prove, although grassroots elections can be used as potential entry points for external actors seeking political leverage. However, technological progress and geopolitical tensions appear to have amplified the scale, complexity and nature of such acts, with AI and non-state actors adding further complications. Indeed, foreign interference can take many forms, such as disinformation campaigns, illicit funding of election actors, and cyberattacks, often navigating in the grey area between interference and influence. Many domestic actors also use the same hybrid tools, making it even more complicated to attribute an attack to a specific group.

1. L: Chamber of Local Authorities / R: Chamber of Regions.
EPP/CCE: European People's Party Group in the Congress.
SOC/G/PD: Group of Socialists, Greens and Progressive Democrats.
ILDG: Independent Liberal and Democratic Group.
ECR: European Conservatives and Reformists Group.
NR: Members not belonging to a political group of the Congress.

Addressing these risks require a comprehensive and balanced approach and the Congress recommends supporting further research on foreign interference in local and regional elections, building resilience of local authorities and strengthening party and campaign finance regulations. Careful approaches are also needed to protect human rights, notably the freedom of expression, and overly restrictive foreign influence laws which could harm civil society should be avoided. Last but not least, facing this multifaceted trend, public awareness remains one of the best forms of protection against foreign interference at all levels of government and the Congress recommends encouraging open debate and promoting voter and candidate education to counter these threats.

**RECOMMENDATION 525 (2025)[2]**

1. The Congress of Local and Regional Authorities of the Council of Europe ("the Congress") refers to:

a. the European Charter of Local Self-Government (ETS No. 122) and its Additional Protocol on the right to participate in the affairs of a local authority (CETS No. 207);

b. Recommendation (2003)4 of the Committee of Ministers on common rules against corruption in the funding of political parties and electoral campaigns;

c. Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting;

d. the Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States (2022);

e. Resolution 2390 (2021) "Transparency and regulation of donations to political parties and electoral campaigns from foreign donors" of the Parliamentary Assembly of the Council of Europe;

f. the Venice Commission Code of Good Practice in Electoral Matters (2002), the Venice Commission, Guidelines on Political Party Regulation, (Second Edition, 2020) and its Opinion on the Prohibition of Financial Contributions to Political Parties from Foreign Sources (2006);

g. Congress Recommendation 518 (2024) "Recurring issues based on assessments resulting from Congress monitoring of the European Charter of Local Self-Government and election observation missions (reference period 2021-2024)";

h. Congress Recommendation 498 (2023) "Local and regional media: watchdogs of democracy, guardians of community cohesion";

i. Congress Recommendation 478 (2022) "Hate speech and fake news: the impact on working conditions of local and regional elected representatives";

j. the Reykjavik Declaration following the Fourth Summit of Heads of States and Government of the Council of Europe (2023), reaffirming the commitment "to hold elections and referenda in accordance with international standards and take all appropriate measures against any interference in electoral systems and processes", and the revised Priorities of the Congress for 2021-2026;

k. United Nations Sustainable Development Goal 16: Peace, Justice and Strong Institutions; Target 16.7: Ensure responsive, inclusive, participatory and representative decision-making at all levels.

2. The Congress points out that:

a. local and regional elections, while attracting modest interest from authoritarian actors, are not immune to the threat of foreign interference in electoral processes to influence the results of an election, via instances of disinformation, opportunistic cyber-attacks and illicit funding. Despite foreign interference being an old and complex phenomenon, recent geopolitical changes and new technological developments have increased the scale, the number of involved actors and the reach of such actions, making it even harder to attribute these attacks to a state actor;

b. grassroots elections should be decided by the voters residing in a community and having the right to participate in the affairs of a local authority and therefore, national, regional and local authorities should take steps to protect the integrity of electoral processes and to ensure that voters form their opinion free from interference and according to their convictions and have the freedom to express such opinion on election day;

2 Debated and adopted by the Congress on 26 March 2025 (see document CG(2025)48-10, explanatory memorandum), rapporteur: Stewart DICKSON, United Kingdom (R, ILDG).

c. while refraining from overemphasising the issue and feeding narratives about rigged electoral systems, a careful examination of recent cases reveals the emergence of many challenges in the handling of potential foreign interference, such as the corrosive effect of small incidents, the increasing manipulation of the concept for political purposes, the growing importance of non-state actors (private companies, individuals, transnational groups, etc) and domestic actors and the potential multiplier that artificial intelligence could represent.

3. In light of the foregoing, the Congress invites the Committee of Ministers to call on member States to:

a. increase efforts to gather scientific and technical knowledge about the issue of foreign interference prior to, during and after local and regional electoral processes, especially in highly contested elections;

b. acknowledge the potential risks associated with foreign interference in local and regional elections and support local and regional authorities in developing infrastructures and expertise to deal with potential threats and disruption;

c. strengthen political party and campaign finance regulations and oversight to prevent illicit funding of contestants by foreign donors and if not already the case, consider prohibiting foreign and anonymous donations to both political parties and candidates, including in local and regional elections;

d. explore ways of fostering open debate at local and regional levels, work towards debunking alternative narratives and addressing the impact of alternative information environments;

e. reinforce behavioural change by promoting voter education and awareness, in particular of new voters, or from vulnerable groups, to build capacity to identify deceptive foreign information manipulation and to encourage critical thinking, in collaboration with civil society and political parties;

f. promote capacity-building of local and regional authorities, in particular lower-level election administration bodies, on cyber security related to various aspects of the electoral process, in particular to voter registers and results management, in order to detect, understand and counter new threats to the integrity of elections;

g. build the capacities of political parties and candidates in local and regional elections to detect and prevent foreign interferences and protect their systems potential cyberattacks;

h. refrain from taking hasty measures such as enacting overly restrictive foreign influence laws, that could clearly jeopardise certain actors, including civil society, and support fact-based journalism, including in minority languages;

i. avoid holding local and regional elections on the same day as national ones, to better monitor and protect these elections from large-scale malicious operations.

4. The Congress calls on the Committee of Ministers, the Parliamentary Assembly and other relevant institutions of the Council of Europe to take account of this recommendation and of the accompanying explanatory memorandum in their activities relating to member States.

**RESOLUTION 508 (2025)[3]**

1. The Congress of Local and Regional Authorities of the Council of Europe ("the Congress") refers to:

a. the European Charter of Local Self-Government (ETS No. 122) and its Additional Protocol on the right to participate in the affairs of a local authority (CETS No. 207);

b. Recommendation (2003)4 of the Committee of Ministers on common rules against corruption in the funding of political parties and electoral campaigns;

c. Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting;

d. the Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States (2022);

e. Resolution 2390 (2021) "Transparency and regulation of donations to political parties and electoral campaigns from foreign donors" of the Parliamentary Assembly of the Council of Europe;

f. the Venice Commission Code of Good Practice in Electoral Matters (2002), the Venice Commission, Guidelines on Political Party Regulation, (Second Edition, 2020) and its Opinion on the Prohibition of Financial Contributions to Political Parties from Foreign Sources (2006);

g. Congress Resolution 505 (2024) "Recurring issues based on assessments resulting from Congress monitoring of the European Charter of Local Self-Government and election observation missions (reference period 2021-2024)";

h. Congress Resolution 496 (2023) "Local and regional media: watchdogs of democracy, guardians of community cohesion";

i. Congress Resolution 485 (2022) "Hate speech and fake news: the impact on working conditions of local and regional elected representatives";

j. the Reykjavik Declaration following the Fourth Summit of Heads of States and Government of the Council of Europe (2023), reaffirming the commitment "to hold elections and referenda in accordance with international standards and take all appropriate measures against any interference in electoral systems and processes", and revised Priorities of the Congress for 2021-2026;

k. United Nations Sustainable Development Goal 16: Peace, Justice and Strong Institutions; Target 16.7: Ensure responsive, inclusive, participatory and representative decision-making at all levels.

2. The Congress points out that:

a. local and regional elections, while attracting modest interest from authoritarian actors, are not immune to the threat of foreign interference in electoral processes to influence the results of an election, via instances of disinformation, opportunistic cyber-attacks and illicit funding. Despite foreign interference being an old and complex phenomenon, recent geopolitical changes and new technological developments have increased the scale, the number of involved actors and the reach of such actions, making it even harder to attribute these attacks to a state actor;

b. grassroots elections should be decided by the voters residing in a community and having the right to participate in the affairs of a local authority and therefore, national, regional and local authorities should take steps to protect the integrity of electoral processes and to ensure that voters form their opinion free from interference and according to their convictions and have the freedom to express such opinion on election day;

3 Debated and adopted by the Congress on 26 March 2025 (see document CG(2025)48-10, explanatory memorandum), rapporteur: Stewart DICKSON, United Kingdom (R, ILDG).

c. while refraining from overemphasising the issue and feeding narratives about rigged electoral systems, a careful examination of recent cases reveals the emergence of many challenges in the handling of potential foreign interference, such as the corrosive effect of small incidents, the increasing manipulation of the concept for political purposes, the growing importance of non-state actors (private companies, individuals, transnational groups, etc) and domestic actors and the potential multiplier that artificial intelligence could represent.

3. In the light of the foregoing, the Congress underlines the importance of adopting a coordinated approach and:

a. calls on its members to take into consideration in their activities the potential risks related to foreign interference in electoral processes at local and regional levels, promote voter education and develop tools to support local and regional authorities to effectively counter this issue;

b. invites the Monitoring Committee to draw attention to this issue when contributing to future reviews of the Venice Commission Rule of Law Checklist and to systematically introduce a dedicated section in Congress election observation reports;

c. invites the Governance Committee to mainstream this issue when developing or contributing to activities related to corruption at local and regional levels, including when contributing to the GRECO's sixth round of evaluations on local and regional corruption;

4. On the basis of this document, the Congress commits itself to continued co-operation with the Committee of Ministers, the Parliamentary Assembly and the Venice Commission as well as with international partner organisations in order to collect, compare and evaluate examples of good practice related to foreign interference in electoral processes.

## EXPLANATORY MEMORANDUM[4]

## I. INTRODUCTORY REMARKS

1. The Congress has long held the conviction that local and regional elections must be decided solely by voters residing in a community and therefore who have a genuine link with their place of residence.[5] The citizens' right to exercise their democratic choice is the foundation of political participation at local and regional levels and in many ways, foreign interference in local and regional elections jeopardises this choice in free elections. While foreign interference at national level has attracted more dedicated attention, Congress observations indicate that local and regional elections are emerging as equally susceptible to these attempts. Indeed, the growing relevance of local and regional elections in the overall electoral landscape increases their exposure to acts of foreign and transnational interference. As guardian of grassroots democracy, the Congress is therefore committed to protect the ability of citizens to form an opinion and express their votes in local and regional elections (and referendums) without interference.

2. In 2023, Heads of States and Governments of the Council of Europe adopted the Reykjavik Declaration, which included a strong recommitment to free and fair elections. The Principles for Democracy of Reykjavik stated that States recommitted to hold elections and referenda in accordance with international standards and take all appropriate measures against any interference in electoral systems and processes. Elections are to be grounded in respect for relevant human rights standards, especially freedom of expression, freedom of assembly and freedom of association, including for the creation of political parties and associations in accordance with national and international standards.

3. Foreign interference in electoral processes is not a new phenomenon, but recent developments, including the expansion of new technologies and geopolitical crises, have permitted a sharp increase in the scale and nature of such endeavours, with significant recent examples in elections in the Republic of Moldova, Ukraine, France, Montenegro, the UK, and elsewhere in Council of Europe member States and beyond. With the 2022 war of aggression of the Russian Federation against Ukraine, further polarisation of the geopolitical landscape and the growing technical skills of some foreign actors have clearly contributed to more unpredictable outcomes, including in local and regional electoral processes. This in particular in a new era of geopolitical tensions, where malevolent actors are looking for "entry doors" to increase their influence beyond national boundaries.

4. Based on its experience in observing elections, the Congress is aware that local and regional elections are not immune to electoral corruption and disinformation of different types. In fact, these elections are often a first step to gain access to some political legitimacy and responsibilities and can therefore constitute a good entry point for foreign interference in decision-making processes. Specifically, local and regional elections can provide a good access to funds and networks.[6] Moreover, as local and regional elections are often held on the same day than national or European Parliament elections, they may also be vulnerable to large-scale attacks and targeted campaigns.[7]

5. Such attacks jeopardise several fundamental rights guaranteed by the ECHR and are detrimental to local and regional democracy, as foreign interference runs counter to the European Charter of Local Self-Government (hereafter the Charter), its Additional Protocol and the European electoral heritage detailed in the Venice Commission's Code of Good Practice on Electoral Matters (see below). Free suffrage can be particularly compromised in its two key aspects: the free formation of the elector's

4 Prepared with the contribution of Dr Christina Binder, Austria, member of the Congress Group of Independent Experts.
5 Article 4.1 of the Additional Protocol to the European Charter of Local-Self-Government on the right to participate in the affairs of a local authority
6 In the US and Canada, several high-profile recent cases of alleged financial interferences in municipal elections have been noted, related to the People's Republic of China's interference. Mayor Adams of New York City was indicted in July 2024 in a foreign influence scheme involving six countries, See William K. Rashbaum, Dana Rubinstein and Michael Rothfeld, U.S. Inquiry Into N.Y. Mayor's Foreign Ties Said to Include 6 Countries, New York Times, 23 September 2024. In Canada, a public enquiry on potential meddling has been established in 2024 and some of the investigated cases relate to provincial and municipal elections. See Michael Murphy, Foreign interference could affect municipal elections, too. Here are 2 ways to reduce it, The Conversation, 26 June 2024,
7 The Congress has consistently recommended holding local and regional elections on a different day than national ones, as a way to reinforce local democracy but it seems that having a separate election day for grassroot elections could also allow members States to better monitor and protect local and regional electoral processes from large-scale malign operations.

opinion (interference by spreading disinformation, influencing political parties or electoral campaigns), and the free expression of this opinion (interference by attacking the electoral infrastructure). Furthermore, on the long run, interferences, not unlike domestic violations, can distort the information environment and jeopardise the trust voters place in democratic processes.

6. The Council of Europe is taking these developments into account in its work on the electoral cycle. The Committee of Ministers approached the issue of foreign funding in its Recommendation (2003)4, on common rules against corruption in the funding of political parties and electoral campaigns, while the Venice Commission addressed some aspects of foreign interference in its Code of Good Practice in Electoral Matters (2002), its Guidelines on Political Party Regulation (Second Edition, 2020) and its Opinion on the Prohibition of Financial Contributions to Political Parties from Foreign Sources (2006). In addition, the Parliamentary Assembly of the Council of Europe Resolution on the Transparency and regulation of donations to political parties and electoral campaigns from foreign donors provided useful guidelines, though focusing primarily on the national level.

7. At the same time, there is generally little attention paid to the local level, despite some hotly contested races attracting both national and international attention. Little research has been conducted on this topic and information on potential interferences on these elections is cruelly lacking, also due to the difficulty to detect and prove such cases. Bearing this in mind, comprehensive analysis is needed for member States to address foreign interference in local and regional elections effectively, in line with the Council of Europe standards including the Charter as well as with international standards and best practices.

8. Furthermore, foreign interference also represents a key challenge for the Rule of Law and the Congress regrets the absence of standards at local and regional levels on this matter, leaving large swathes of the electoral processes underregulated and unprotected. Paradoxically, while corruption is often well-assessed at local and regional levels, the same is not true regarding foreign interference. Grassroots elections are often omitted or under-valued compared to national elections in international standards and as a result, suffer from a lack of solid protection.

9. The present Congress report aims at analysing the growing threat of foreign interference in local and regional elections, which undermines democratic principles at subnational level and the right of citizens to freely express their political choices. Despite existing Council of Europe standards on election integrity and Rule of Law, the lack of specific protections at the local level, highlights the urgent need for research, regulation, and stronger safeguards to uphold democratic processes. This report thus seeks to fill this gap at local and regional levels and will draw from examples at all levels of government, as well as applicable international standards, without overamplifying this trend. This transversal report will also explore best practices to mitigate the impact of foreign interference in electoral processes, focusing on enhancing the resilience of domestic actors - local and regional authorities as well as voters and contestants - in elections.

10. This report approaches this topic from various angles. After a brief background (Part II.), the report will examine the various types of foreign electoral interference before, during, and after elections in reliance on concrete examples from local and regional elections in the Council of Europe member states where foreign interference has been proven or credibly alleged (Part III.) and their serious consequences of foreign electoral interference. Part IV will explore the rules of international law at stake and the international (human rights) framework applicable to foreign electoral interference from the perspective of the state aiming to contain/address acts of interference. Part V deals with the specific standards and best practices for each area of foreign interference discussed, likewise drawing on selected domestic best practice examples.

## II. DEFINITION AND BACKGROUND

11. Foreign interference in electoral processes, while not new, appears to have globally increased in the last decade, including in the context of local and regional elections. For this report, foreign interference will be understood as a broad phenomenon, characterised by the following three elements:

- “Interference“, in the meaning of “getting involved“ without being asked to do so.

- "Foreign": While interference with electoral processes may also stem from domestic actors, *foreign* interference is characterised by another state or foreign (i.e. non-national) actor intervening. This creates an international dimension to acts of interference.
- "Electoral process": using the electoral cycle approach, elections are a continuous process. While the time around election day, especially the election campaign, is usually most exposed to acts of (foreign) interference; foreign interferences may take place at any time, such as in-between elections; for instance on issues with voter registers or illicit funding of political parties.

12. In this context, one could arguably distinguish between *interference* and *influence,* with the former constituting more coercive operations while the latter being more subtle – designed to influence and persuade rather than coerce.[8] In both cases, it remains very complex to establish that a type of influence or interference had a significant impact on the electoral results.[9]

13. Foreign interference in electoral processes at local and regional levels is therefore multifaceted, can be regulated or unregulated and carried out by state or non-state actors. While some aspects of these activities constitute criminal or administrative offences in member States, several other activities are unregulated or can even be considered as part of a normal democratic debate, in other member States.

14. For this report, three main types of interference will be distinguished: financial interference, information manipulation and electoral cyberattacks. Still, the tactics employed by foreign actors are diverse and continually evolving, ranging from the corruption of politicians and covert financial backing of candidates/parties, over mis- or disinformation campaigns, to state-sponsored cyberattacks and the manipulation of voting systems. Recent instances of such meddling in national and subnational elections across Council of Europe states like the Republic of Moldova, Ukraine, France and the UK have triggered global concerns, prompting discussions on the vulnerability of electoral systems and the urgent need for robust safeguards. Positively, many local and regional elections are not targeted by foreign interference, but the use of the same tools by domestic actors can be as concerning.[10]

15. Interference in electoral processes by foreign actors or states is an old and relatively common phenomenon. Indeed, first mentions of foreign interferences in electoral processes can be traced back to the pre-modern era as early as in the 13th century's papal elections when European monarchs sought to influence the selection of the new pope.[11] When modern elections with mass electorates began to occur in the late 18th century, they frequently attracted the attention of almost every major power. France, for example, openly intervened in the 1796 U.S. elections in order to prevent the re-election of George Washington.[12] Nazi Germany and Soviet Union likewise attempted to influence elections in the U.S.[13] Later, during the Cold War era, electoral interventions became a common feature of great-power politics. Allegedly, the U.S. and the USSR/Russia (also through the Communist International) intervened 117 times between 1946 and 2000 which makes up about one of every nine competitive national-level elections during this period.[14] This shows that attempts to influence the outcome of an election have been made in particular for strategic interests. Interferences have been conducted by foreign states and other (non-state) actors to expand their leverage beyond the national level.

16. In Europe, many countries still have vested interests in the grassroots elections of their neighbours due to shared history or large diasporas. Such examples are common in former Yugoslavia and the Balkans, as well as in Baltic countries. The line between influence and interference is thin, and some Congress interlocutors have regularly regretted the strong influence of these countries in their local affairs. Many reports of fraudulent voter registration and specific disinformation targeting a minority group have been voiced by NGOs have also been raised, in particular in the Balkans. Such allegations

8 Kristine Berzina and Etiene Soula identify two common elements of foreign interference in politics: their 'malicious intent' and 'lack of transparency', Berzina, K. and Soula, E., Conceptualizing Foreign Interference in Europe, Alliance for Securing Democracy, 18.3.2020.

9 See Venice Commission (2025), Urgent report on the cancellation of election results by constitutional courts.

10 Common Consultancy, Report: Mapping foreign influence on social media before, during, and after the Norwegian municipal council and county elections 2023, 15 January 2024 (available in Norwegian only).

11 Baumgartner, Frederic. 2003. Behind Locked Doors: A History of the Papal Elections. New York: Palgrave, pp. 98–102.

12 DeConde, Alexander, Entangling Alliances: Politics and Diplomacy under George Washington, Duke University Press, 1958.

13 B. W. Hart, Nazis and communists tried it too: Foreign interference in U.S. elections dates back decades, 2019,

14 Levin, Dov H. Meddling in the ballot box: The causes and effects of partisan electoral interventions. Oxford University Press, USA, 2020, Chapter V.

were recently raised during Congress election observation missions to Bosnia and Herzegovina and Podgorica (Montenegro).

17. While threats of interference existed in the past, with advances in information technologies an evolution of strategies is perceptible. Previous instances of foreign interference were characterised in particular by financial influence (vote buying) and isolated instances of information manipulation.[15] New and emerging technologies, including Artificial Intelligence (AI), have led to an unprecedented increase in foreign interferences with elections. Also the rise of social media to the detriment of traditional media channels has contributed thereto.[16] Ongoing technological advancements and a deepening global interconnectivity increase reach and the potentially negative consequences of possible cases of interference.

18. Moreover, geopolitical tensions have added new dimensions in a changed international landscape and a divided multipolar world. Especially Russia's war of aggression against Ukraine has increased the potential and also the actual quantity of attacks – new forms of warfare, including targeted network attacks, are observable and carry growing threat potentials.[17] Through the use of modern technology and global networks, foreign actors increasingly aim to manipulate electoral outcomes while resorting to networks of proxies and actors loosely working under their umbrella, thereby undermining the core tenets of democracy.[18] While the goal of foreign interference has always been to push for one's interest, another more subtle and more permanent goal seems to have emerged recently: to destabilise democratic institutions at all levels of government. Through such destabilisation, some actors perceive fostering mistrust in democratic processes as a potential channel to weaken their opponents. This approach is sometimes called "hybrid warfare"[19] and "hybrid threats".[20]

19. However, the concept of foreign interference remains tainted in controversy, as most allegations are not followed by careful and public examination of evidence available. As a tool to advance strategic interests, most countries are involved in foreign interference in a way or another. The debate arising from the questioning on what type of interference is legitimate or necessary, for instance to support other democratic actors, is a long and well-established one. However, some actions that were widely accepted in the past are now increasingly being labelled as "interference" by national authorities, such as international election observation, a state commenting on the results of the elections in a neighbouring country and even the support to civil society and media. As seen in the recent adoption of many foreign influence laws, the legitimate attempts to protect democratic institutions from foreign interference can turn into a political battlefield, with oppositions to it being labelled "foreign agents". Indeed, this label can be a very powerful tool to discredit a political adversary (or civil society) without having to justify these claims. Furthermore, the recent change of administration in the US, with President Trump accusing USaid of fraud and bias and Head of the US Department of Governmental Efficiency Elon Musk clearly acting as a destabilising actor in UK and German politics, has emboldened some European actors to label NGOs and investigative media as foreign actors in order to suppress criticism.[21]

20. For the local and regional level, the phenomenon of foreign interference has grown in scope and dimension, due to the growing importance of local and regional elections and the fact that the local and

15 Ibid.
16 See the Venice Commission in relation to misinformation, foreign interference with "fake news" e.g. in connection with the 2016 U.S. presidential elections: "This is a new version of the old struggle over the definition of truth, political and financial forces waging propaganda wars with 'fake news' as the main weapon." (Joint Report of the Venice Commission and DGI on Digital Technologies and Elections, 2019, para. 25).
17 Andrej Poleščuk, Veronika Krátka Špalková, Hybrid CoE Research Report 10 Preventing election interference: Selected best practices and recommendations, 2023.
18 The conflict in Ukraine transformed the cyber threat landscape giving rise to cyberattacks against Ukraine but also targeting governmental organisations across Europe which have provided assistance to Ukraine.
19 The term hybrid war was first coined in 2007 by Frank Hoffman, in Conflict in the 21st Century: The Rise of Hybrid Wars, Potomac Institute for Policy Studies, 2007.
20 The EU refers to hybrid threats and defines them as "when, state or non-state, actors seek to exploit the vulnerabilities of the EU to their own advantage by using in a coordinated way a mixture of measures (i.e. diplomatic, military, economic, technological) while remaining below the threshold of formal warfare. Examples are the hindering of democratic decision-making processes by massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors." See European Commission website, Hybrid Threats, (updated in 2024).
21 See Buyuk H. "**Europe's Illiberal Leaders Embrace 'Foreign Agents' Laws as Tool to Stifle Criticism**", Balkan Insight, 25 October 2024.

regional level is a convenient “entry point” for foreign interference especially in times of heightened geopolitical tensions.
These increasingly impact local and regional elections especially in some strategic states, as the Republic of Moldova, Ukraine, Bosnia and Herzegovina and the United-Kingdom (see below Part III).

21. To tackle the phenomenon of foreign interference in electoral processes is challenging for many different reasons. On the one hand, and while it is undeniable that instances of foreign electoral interference may interfere with human rights obligations which a state holds vis-a-vis its population (e.g. the right to free elections, freedom of expression including to receive information,..) and thus require according action, the very effort to restrain foreign electoral interference may itself negatively impact on human rights guarantees, such as the freedoms of expression or association. States thus have to navigate between their obligations to protect and to respect human rights.

22. Another challenge relates to the fact that private actors/intermediaries (as social media outlets, international banks) play a crucial role in information manipulation and the distribution of electoral disinformation. Thus, there is a requirement for regulation of the private sector and the question to what extent private actors may be obliged. To establish the accountability of social media outlets can be tricky, as will be shown. Equally challenging is the participation of local proxies in foreign interference and the use of the techniques described below by domestic actors, which remain the main source of concern for local and regional elections. Indeed, foreign interference is also an opportunistic endeavour and can thrive while relying on networks of affiliated or friendly domestic actors. Finally, due to the hybrid nature of these threats, it is particularly challenging to detect and prove such interferences, as the line may be blurred between foreign meddling and domestic corruption.

23. However, while this report focuses on foreign interferences, the Congress points out that threats to the integrity of local and regional elections in Europe remain overwhelmingly domestic.[22] This report attempts at assessing this emerging issue but is well aware that overamplifying the threats of foreign interferences can contribute to the creation of the desired alternative environment and jeopardise the trust in democracy. The report will try to remain fact-based, as many claims of foreign interferences are often not clearly established.

## III. TYPES AND EFFECTS OF FOREIGN INTERFERENCE IN LOCAL AND REGIONAL ELECTIONS IN EUROPE

24. While elections can be distorted in many ways, the following part will address the three primary and most common forms of foreign interference in elections: 1) financial interference, 2) information manipulation, and 3) electoral cyberattacks, before, during and after an election. In doing so, it draws (where possible) on local and regional elections in Council of Europe member states and beyond where foreign interference has been proven or credibly alleged. A full Congress report could be dedicated to each of these three types of interference as their effects are very broad, but this section will explore the overarching trends related to this phenomenon.

25. These attacks, even when of limited impact, must be understood in a broader context of democratic backsliding throughout Europe. The corrosive effect of constant small incidents and violations and the progressive construction of an alternative information environment create a long-term threat to local and regional democracy by fostering mistrust, anger and dissent.[23] This report is well aware of the well-documented attempts to influence/interfere in national elections which primarily threatened democratic processes and contributed to undermine the trust of citizens in their institutions such as the 2016 US presidential elections, the 2022 French presidential election and more recently, the alleged widespread interference in the 2024 Moldovan presidential elections and the 2024 Romanian presidential elections. However, as the focus of the report is on grassroots electoral processes, it will only refer to these in a limited manner.

22 Congress Recommendation and Explanatory Memorandum on Recurring issues based on assessments resulting from Congress monitoring of the European Charter of Local Self-Government and election observation missions (reference period 2021-2024).
23 European Union External Action Service, “2nd Report on Foreign Information Manipulation and Interference Threats – A Framework for Networked Defense”, January 2024.

26. The negative effects of foreign electoral interference may thus be significant. At the same time, they depend on the concrete act of interference, its intensity and scale. Taking this distinction into consideration, relevant criteria/factors to assess the seriousness of an act of interference include the following:

- the extent of foreign interference, as regards intensity and scale: Is the foreign interference a country-wide phenomenon or one of limited geographical reach? Is, e.g. financial interference/illicit party funding, an isolated incident or exercised on large-scale and in big numbers? The *quality of interference* may vary as regards the severity of impact: for instance, as regards information manipulation one may ask: what is the extent of mis- or disinformation; are even elements of hate/inflammatory speech involved?[24]
- In terms of methods, what is the degree of interference and coercion? Concerning cyber-attacks, for instance, are forms of electoral infrastructure physically disabled through the attack? In case of information manipulation, what is the accuracy of the information presented? Is there also truthful information involved? At what time of the electoral campaign is the information released – is there still a possibility to rebuke wrong information?
- In terms of effects/consequences: how severe and lasting are the consequences of electoral interference on the election infrastructure, e.g. in case of cyber-attacks? Moreover, how easily can foreign electoral interference be detected and remedied? What is the degree of awareness in the respective states and their population?
- Finally, which human rights are put to detriment through the attack and a state's counter-measures? In light of the case law of the ECtHR, restrictions on the freedom of expression, especially the freedom of the press to e.g. suppress electoral disinformation, may be more difficult to justify for a state than restrictions of the freedom of association when it comes to the foreign funding of political parties.

## 1. Financial interference

27. In nearly all elections observed between 2021 and 2024, the Congress recommended strengthening party and campaign finance legal frameworks and their oversight in order to guarantee a more even playing field between candidates. The Congress was particularly worried by the situation witnessed in the Republic of Moldova in the context of the 2023 local elections, in which illicit foreign funding was particularly present. Indeed, this aspect of electoral processes often remains overlooked, can be circumvented by both domestic and foreign actors and fails to provide equal conditions for candidates and full transparency for the voters. This situation tends to undermine the fairness and/or integrity of political competition, to distort the will of voters and to threaten some aspects of the electoral process.[25]

28. Financial participation from foreign actors in local and regional elections could be considered as a type of political participation from actors not entitled to vote nor maintaining a genuine link with these subnational units, which is not in line with the Additional Protocol to the Charter of Local Self-Government. Several names cohabit to qualify this phenomenon (malign foreign funding, illicit foreign funding, etc). As other types of interference, it is a very difficult to track, prove and attribute to a certain country a case of financial interference. Furthermore, with the increased involvement of non-state actors (e.g. private companies, individuals, oligarchs, churches, proxy organisations or parties), such attribution can be even more challenging. However, it is clear that authoritarian regimes do not always strongly coordinate actions between their citizens but can also informally encourage (and benefit from) their activities.

29. Targeted clandestine financial support for specific candidates and parties can not only distort the playing field of electoral competition,[26] but it can allow hostile foreign actors to influence and promote

24 "Disinformation" refers to verifiably false, inaccurate or misleading information deliberately created and disseminated to cause harm or pursue economic or political gain by deceiving the public. Committee of Ministers Recommendation CM/Rec(2022)12, para. 7. of the Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States

25 Josh Rudolph and Thomas Morley, Covert Foreign Money: Financial Loopholes Exploited by Authoritarians to Fund Political Interference in Democracies, (2020), p. 7,

26 According to OSCE/ODIHR, claims of a significant influx of illicit funds, mainly from abroad, and monetary incentives used to influence voters' choices distorted the campaign and threatened the level playing field in the Moldovan 2023 local elections. In

specific policy agendas, extending their leverage well beyond election periods. This may constrain institutions and prove detrimental to grassroots democracy, as it raises questions of accountability of the elected representatives.[27]

30. While a variety of practices, regulations and funding caps cohabit in Europe, the Congress observed that unregulated money in grassroots politics can lead to undue influence and corruption, as even a few thousand euros for promotion can give a substantial advantage to a candidate in a great number of elections for local administrations. Foreign illicit funding (similarly to domestic illegal funding) is therefore even harder to spot when regulations are lacking, or not systematically applied and malicious actors can find many ways to circumvent such regulations.

31. As noted in the Parliamentary Assembly Resolution on Transparency and regulation of donations to political parties and electoral campaigns from foreign donors, regulations, even when they do exist, can be deliberately circumvented via : 1) by contributing in-kind instead of in-cash; 2) by providing loans; 3) by contributing in-kind or in-cash to politicians and political candidates instead of political parties and electoral campaigns; 4) via intermediary individuals or companies; 5) via straw companies deliberately created to establish a legal presence in the target country; 6) by contributing to foundations, associations, charities, religious organisations and other non-profit or non-governmental organisations with the aim to covertly benefiting a political party or electoral campaign, thus diverting the funding from the original goal of a non-profit or non-governmental organisation; 7) by using cryptocurrencies; 8) by contributing anonymously or by exploiting de-minimis or cash rules; 9) by concealing the foreign contribution in a business operation, particularly in the energy or natural resources sector.[28]

32. While this list is not exhaustive as malign actors often quickly identify new loopholes in regulations, many of the above-mentioned issues have been observed in the context of regional and municipal elections. Malicious foreign actors can therefore seek to influence the elections through financial contributions to certain candidates and political parties or by financing specific election campaigns. Such election interventions through financial channels may consist in direct contributions, loans, or other financially beneficial transactions, occurring both at central and local government levels and are not limited to the official campaign period. Additionally, support may extend beyond monetary donations to include in-kind contributions, such as providing free media space or airtime for promoting a specific candidate or party.[29] The Russian Federation has notably gained widespread notoriety for extensively employing financial instruments and in-kind contributions from actors with ties to the state to bolster political parties or individual candidates on a global scale, but is not the only foreign actor involved in funding political actors.[30]

33. Attempts to buy votes, despite being outright illegal in nearly all member States,[31] have also been noted in a limited but worrying number of elections. Vote buying often targets individuals with lower income levels who may be more susceptible to monetary or in-kind rewards, such as food, energy or medicine.[32] The buying or recruitment of candidates may comprise the payment of parties to liberate space on the ballots for specific candidates or various types of corruption when (monetary) incentives are offered for the promotion of a particular policy.

---

the lead-up to the elections, the authorities made several claims of foreign interference and cited its detrimental effect on national security. OSCE/ODIHR, Final Election Observation Report, 2023 Local Elections in Moldova, 2023, p. 15.

27 The Congress concluded in relation to the Moldovan 2023 local elections that "the numerous and credible reports of electoral corruption, illegal campaign and party financing, and interference of foreign and/or criminal groups with a view to distorting the will of voters in the local elections considerably strained the institutions and were detrimental to local democracy." Congress of Local and Regional Authorities, Election Observation Report on the 2023 Local Elections in the Republic of Moldova, 2023, Recommendation 5.a.

28 Seven types of malign political party finance were identified by Rudolph and Morley, *Op.Cit*: in-kind contributions, that is intangible or difficult-to-value benefits for political campaigns; straw donors with domestic citizenship or covert agents; shell companies and businesses; non-profit organizations, which are not required to disclose the identity of their donors; online political advertisements, whose regulations are generally looser than for the print and broadcasting media; media outlets funded or supported from abroad; emerging technologies, such as cryptocurrencies and cashless payments, offering anonymity"

29 Schmitt, G., Mazza, M., Blinding the Enemy: CCP Interference in Taiwan's Democracy, Global Taiwan Institute, October 2019,.

30 See Edoardo BRESSANELLI, Investing in destabilisation: How foreign money is used to undermine democracy in the EU (2020), European Parliament Think Tank Study. See also Congress Election Observation Report on the 2023 Local Elections in the Republic of Moldova, 2023.

31 It undermines voter autonomy and creates dependencies, often involving a network of intermediaries who negotiate with voters. Joseph, O., Vashchanka, V., Vote Buying: International IDEA Electoral Processes Primer 2, 2022,

32 In some cases, vote buying strategically targets apathetic voters, highlighting the complexity of these manipulative tactics, which can be utilized by both domestic and foreign actors. See e.g. Jensen, P.S., Justesen, M.K., 'Poverty and Vote Buying: Survey-Based Evidence from Africa', Electoral Studies, Vol. 33, March 2014, pp. 220–232.

34. Instances of alleged vote and candidate buying have primarily been observed in domestic politics, typically involving local candidates and their intermediaries who offer incentives to constituents in exchange for their votes.[33] However, the line can be blurred between domestic and foreign actors in such cases, as a foreign stakeholder can financially support a domestic proxy by providing funds of unknown origin, access to the banking system and strategic support and protection from prosecution. One particularly worrying case of such support at local and regional levels has been well-documented in the Republic of Moldova, where former oligarch Ilan SHOR, exiled in Israel due to his involvement in one of the biggest corruption scandals in the history of the country and endorsed by Moscow, has progressively set up a clientelist system of financial rewards to capture local and regional administrations to the benefit of the SHOR party. First elected as mayor of Orhei in 2015, he used his wealth to open food markets with reduced prices for his supporters, raised salaries and injected money in the city's infrastructure from unknown sources, a model replicated in Taraclia and the Autonomous Territorial Unit of Gagauzia (hereafter ATU Gagauzia). Later condemned for corruption and the SHOR party declared unconstitutional, Mr SHOR set up a network of proxy parties and continued to inundate local politics with foreign funds (cash, credit cards and loans) from unknown sources in the November 2023 general local elections and the April 2023 governor elections in the ATU Gagauzia.[34]

35. The Congress noted in its election observation report that the 2023 local elections "unfolded under challenging circumstances and widespread allegations of foreign interference and hybrid warfare, at a time of decisive choices between a stronger pro-European stance or a resolutely pro-Russian one."[35] Specifically, the Congress referred to attempts to illegally finance political parties and campaigns, which have shaped the country's political landscape in recent years and escalated dramatically in 2022-23. Almost all Congress interlocutors lamented the numerous, persistent, and widespread allegations of vote buying and electoral corruption emanating from satellites of the Shor party,[36] such as the new Chance party founded shortly before the elections.[37] These attempts were often accompanied by strong suspicions of interference from foreign actors in local politics, as was already established in the Transnistrian region of the Republic of Moldova and ATU Gagauzia, yet the origin of these funds remained well camouflaged.[38] During the following 2024 Moldovan presidential election and constitutional referendum, similar credible evidence of external financial interference emerged, including illicit monetary incentives aimed at influencing voters.[39]

36. The 2021 local elections in Niksic also constituted a turning point in Montenegro, as neighbouring Serbia became strongly involved in the local campaign. The presence of personalities close to or members of the SNS, the ruling party in Serbia, raised concern and some of them were detained (and even banned from entering the country) on suspicion of bringing in money to buy votes. After promising it during the campaign, the City of Belgrade made a two million euros donation to Niksic.[40]

37. Furthermore, foreign financial support of political entities is not limited to the electoral period. As noted in 2021 in a study commissioned by the European Parliament, some major political parties, such as the *Rassemblement National* in France,[41] *Lega* in Italy, Freedom Party in Austria and the Brexit Leave campaign have been under scrutiny/investigation in their respective countries for cases of foreign

33 See e.g. Allina-Pisano, J., 'Social Contracts and Authoritarian Projects in Post-Soviet Space: The Use of Administrative Resource', Communist and Post-Communist Studies, Vol. 43, No. 4, 1 December, 2010, pp. 373–382.
34 Matveyenko J., Assessing the Impact of Disinformation on Minority Communities in Moldova, December 2023.
35 Congress, Election Observation Report on the 2023 Local Elections in the Republic of Moldova, 2023, para. 11.
36 The SHOR Party is a populist political party in Moldova founded by Ilan Shor in 1998 as the Socio-Political Movement "Equality" and renamed to its current name in 2016. The party was banned in 2023 as "unconstitutional".
37 A new political party called "Chance" was established in 2003 but later de-registered as a political party two days before the local elections in November amid claims of accepting illegal funds from abroad.
38 Regarding the ATU Gagauzia elections, see Victoria Olari, "A Russian footprint in Moldovan regional elections," Digital Forensic Research Lab, 12 May 2023, and Andrew Higgins, "Cash, Mules and Paid Protests: How a Fraudster Seized an Ethnic Enclave," New York Times, 24 September 2023,
39 For instance, ODIHR's mission learned of text messages, including one received by an ODIHR observer two days before election day, offering payment to promote a "no" vote in the referendum via social media. Additionally, unregistered actors, both online and offline, were observed actively campaigning on referendum issues. OSCE/ODIHR election observation report, presidential and parliamentary elections in Moldova, 2024, pp. 13-14. See also, News Maker 23 April 2024, "Shor Couriers brought over 20 million Lei from Moscow in a single day. The money was intended to finance political parties",
40 See Center for Democratic Transition (2024), "Foreign influences on the electoral process in Montenegro 2016–2023 – Part I"
41 Note that this party also received a loan by Hungarian bank close to Hungarian PM Orban ahead of the 2022 elections, as revealed by the Financial Times. Marine Le Pen received loan from Hungarian bank with ties to Viktor Orban 9 March 2022,

funding or generous loans from banks affiliated in foreign countries.[42] In the context of the 2017 Catalonian Independence Referendum, the Organized Crime and Corruption investigative network alleged financial promises were made by Russian affiliates to Catalonian leaders to support their independentist claims, if the outcome of the referendum was positive.[43] The Spanish judiciary is still investigating these claims.[44]

38. Financial support is very challenging to track and even when the legislation exists, some countries are not always well equipped to systematically monitor bank accounts and transactions, in particular in local and regional elections, where the number of candidates is multiplied. Indeed, institutions in charge of the monitoring can suffer from being understaffed or from political pressure to perform their tasks. In Montenegro or in Bosnia and Herzegovina, the Congress observers noted serious issues with the staffing of institutions in charge of evaluating the financial reports, which often leads to delay in making the reports public or sanctioning political actors.

39. Finally, foreign financial support can also be very challenging to track as foreign powers can resort to foundations, associations or organisations targeting their diasporas or communities of the same ethnic background to push for their own agenda. From funding social and cultural projects in municipalities or regions in order to show their support to some candidates, this type of activity stands on the brink between interference and influence. For instance, in 2019, the opening of an integration centre by Azerbaijani officials in Marneuli (Georgia) and support to a mayoral candidate and the ruling party was considered by some observers as an attempt to influence the vote of the Azeri community in the city.[45] Foreign influence in the Balkans (Serbia, Bosnia and Herzegovina and Montenegro in particular) is said to be using this technique as well, relying both on cultural centres and religious authorities including the Serbian Orthodox Church.[46] In 2024, some interlocutors of the Congress election observation mission to observe the elections in Podgorica alleged that the endorsement by the Church of one political party could amount to a foreign influence attempt. Such accusations have been voiced also regarding other religious authorities placed under the responsibility of a foreign power. A 2023 report on the activities of the parliamentary committee on intelligence of the French National Assembly[47] alleged that many mosques resorting to the “seconded” imam practice (imam detached by the religious authorities of another country) or relying on foreign financing had enabled Türkiye to exert its political and religious influence on Islam in France, through the Ditib, an offshoot of the Turkish Ministry of Religious Affairs, the Diyanet. It represented then around 250 associations and 120 imams of Turkish origin under the detached imam system.

### 2. Information manipulation[48], including on internet (social media/new technologies)

40. Information manipulation is a global trend affecting all aspects of citizens’ lives, including local and regional democracy. While information on online and social media flow more freely, it does not entail that it is completely unregulated or not submitted to regulations. The Congress has previously acknowledged in a report its impact on local and regional elected representatives,[49] but while most information manipulation originates from domestic sources, it has become increasingly clear that foreign actors are also very much involved in pushing some narratives detrimental to local democracy, including through bots and trolls. Indeed, information manipulation strives to influence voting behaviours in both targeted and long-term ways. Targeted practices involve focusing on specific populations and relevant

42 See Investing in destabilisation: How foreign money is used to undermine democracy in the EU, Op.cit.
43 Fueling Secession, Promising Bitcoins: How a Russian Operator Urged Catalonian Leaders to Break With Madrid, Organised Crime and Corruption Reporting Project, 8 May 2022.
44 Spain Extends Probe into Russian Involvement in Catalonian Independence Plans, Organised Crime and Corruption Reporting Project, 28 January 2024 and Michael Schwirtz and José Bautista, Married Kremlin Spies, a Shadowy Mission to Moscow and Unrest in Catalonia The New York Times, September 2021.
45 See Eurasia Net, Georgians allege Azerbaijan interfering in their local elections, 15 May 2019.
46 See Wouter Zweers, Niels Drost & Baptiste Henry, Little substance, considerable impact Russian influence in Serbia, Bosnia and Herzegovina, and Montenegro, Cligendael, 2023.
47 Assemblée Nationale, Sacha Houlié (Rapporteur), Rapport relatif à l’activité de la délégation parlementaire au renseignement pour l’année 2022-2023, n° 1454, déposé le jeudi 29 juin 2023.
48 Joint Report of the Venice Commission and DGI on Digital Technologies and Elections, para. 39 “information disorder“ distinguishes between: Mis-information, that is sharing false information, but without the intent of causing harm; Dis-information, which stands for knowingly sharing false information with the intent to harm; and Mal-information, which describes genuine information shared with the intent to cause harm, often by disclosing information from the private sphere into the public sphere. Especially the latter two (dis-information, mal-information) are of relevance in cases of foreign influence.
49 See Congress Recommendation and Explanatory Memorandum, Hate speech and fake news: the impact on working conditions of local and regional elected representatives, October 2022.

political topics during election periods, while broader practices include exacerbating societal anxieties,[50] promoting polarising narratives, and dehumanising certain social groups throughout the electoral cycle[51] and consequently also in periods between elections.[52] All this hinders informed choices of voters; at times involving hate speech.

41. However, in the context of elections, it is important to remember that, as the Venice Commission stated in the 2025 Urgent report on the cancellation of election results by constitutional courts "electoral campaigns are in essence information campaigns by the candidates designed to convince the voters" and that therefore, some content, including value judgment and negative campaigning, shared by political contestants can sometimes be labelled as disinformation but fall under the candidate's freedom of expression, unless they exceed permissible limits.[53]

42. Traditional media is one clear mean to push alternative narratives with public broadcasters being the most common tool to do so. RT and Sputnik channels are long known for spreading false or misleading news in the context of elections and were banned from the EU following the beginning of the war of aggression against Ukraine but are not banned in other European countries.[54] Private channels loosely affiliated with foreign actors are also a source of concern during local and regional elections and transparency over the ownership of such channels is often lacking, therefore making it difficult to prove foreign ownership.[55] In the context of the 2021 local elections in Niksic (Montenegro), Serbian TV channels, [56] TV Happy in particular, covered extensively the contest through dedicated programmes such as "the battle for Niksic", while not respecting provisions applicable to the fairness of media coverage of election campaigns and broadcasting ethnic-based hatred and racist slurs.[57] Such allegations were also voiced later in Podgorica and Budva.

43. Moreover, social media manipulation campaigns can have long-term effects that extend beyond their immediate objectives of swaying or confusing public opinion, such as the erosion of trust in democratic institutions and electoral processes, but attribution to a user, a candidate let alone a foreign power is particularly complex.[58] By instilling doubt and suspicion about the integrity of the electoral system, foreign actors can therewith weaken the foundations of democratic governance, fostering instability and division within societies at all levels of government. While the internet provides for an open space to report violations and allows for in-depth scrutiny, it also amplifies fake reports or baseless claims, which can be voluntary or based on misunderstanding of electoral procedures.[59] Due to the high number of social media platforms and challenges in moderating their content (Facebook/Meta, X/Twitter, Telegram, Vkontakte, Youtube, Tiktok and smaller forums), the constant struggle to remove content is increasingly hindered. Recent backtracking on content moderation by platform owners of Meta and X are at odds with efforts to fight against disinformation online. By doing so, 'they create a

50 For instance, in the context of the 2023 local elections in the Republic of Moldova, the SHOR party, supported by foreign accounts, leveraged the Jewish identity of its founder to connect ideologically with Gagauz, Bulgarians, and other ethnic groups by comparing the Sandu government to Nazi Germany and suggesting that genocide and ethnic violence may occur against all minority groups in Moldova. See Assessing the Impact of Disinformation on Minority Communities in Moldova, December 2023.
51 A report by investigative outlets Telex and Direkt36 alleged that Hungarian authorities released political advertisements promoting Hungarian government's anti-migrant rhetoric on Youtube in numerous neighbouring countries, including ahead of local elections in Italy and Germany in 2023. Panyi Szabolcs, How Orbán flooded Central Europe with millions of online ads during election season, Direkt 36 and Telex, 2024.
52 E.g., a disinformation campaign conducted by Russia propagated false information regarding the misconduct of Ukrainians in Europe, demonstrating the broader repercussions of such strategies. Neidhardt, A.H., Disinformation on Refugees from Ukraine: Boosting Europe's Resilience after Russia's Invasion, Foundation for European Progressive Studies, 2022,
53 See Venice Commission (2025), Urgent report on the cancellation of election results by constitutional courts.
54 European Council, Press Release "EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU", 2 March 2022.
55 See for instance, Resource Center on Media Freedom in Europe, Foreign media ownership in Europe, 2018 and European Audiovisual Observatory, Transparency of media ownership, 2021.
56 See Center for Democratic Transition (2024), "Foreign influences on the electoral process in Montenegro 2016–2023 – Part I"
57 The Congress was also made aware of these issues in the context of the 2024 Podgorica elections. Vujovic Z. (ed.), "Electoral Reform in Montenegro - Recommendations for Improvement", Centre for Monitoring and Research (CEMI), 25 March 2024.
58 These campaigns can specifically undermine confidence in ballot counting procedures, election officials, and alternative voting methods. See e.g. Brennan, G., Lomasky, L., eds., 'The Logic of Electoral Choice', Democracy and Decision, 1st ed., Cambridge University Press, Cambridge, 1993, pp. 19–31.
59 See Birch, S., & Elsafoury, F. (2017). Fraud, plot, or collective delusion? Social media and perceptions of electoral misconduct in the 2014 Scottish independence referendum. *Election Law Journal: Rules, Politics, and Policy*, *16*(4), 470-484.

vacuum where disinformation thrives unchecked and the harm to democracy is deep," stated the Council of Europe Commissioner for Human Rights, Michael O'Flaherty.[60]

44. As a report of the European Union External Action Service elaborated, "Foreign Information Manipulation and Interference (FIMI) targets all aspects of our societies; even though many individual FIMI incidents remain limited in their impact, the constant, daily, manipulative behaviour attempting to undermine our societies, trust in democracy and the international, rules-based order can have a long-term corrosive effect. Foreign actors deploy information manipulation and interference as a systematic tool of their foreign policy, targeting in particular vulnerable groups and attacking journalists and civil society, as well as undermining trust in democratic processes".[61]

45. Furthermore, hostile foreign actors have engaged in information manipulation, attempting to shape public opinions. Their strategies often involve coordinated campaigns through various media channels, including social media, to disseminate content designed to appear as if it originates from the target country.[62] While information manipulation has long been a feature of the international system and predates the internet era, advancements in technology have lowered costs and expanded the scope, reach, and speed of information transmission.[63] Social media platforms, in particular, allow for audience segmentation and targeted messaging with minimal regulation.[64] The 2020 Global Inventory of Organized Social Media Manipulation report of the University of Oxford alleged that 81 countries had used social media to spread computational propaganda and disinformation, often resorting to private companies to do so.[65]

46. One emerging aspect of information manipulation is the use of artificial intelligence in such endeavours, via the creation of bots, algorithms and more particularly deepfake. However, at the time of preparation of this report, little evidence of the use of AI (and its preference over reusing more classic memes and photo edits) has been gathered and thus, this report will not be able to go in depths, while noting risks associated with the deployment of AI. Artificial intelligence could indeed be a multiplier of deceptive content, but could also benefits people fighting disinformation, by developing tools to track inauthentic behaviour.[66]

47. Social media campaigns may serve as tools for shaping public opinion in the lead-up to elections.[67] Coordinated influence operations frequently employ deceptive tactics to make their messages appear genuine to the target audience; sometimes relying on AI-powered tools and language models which allow messages to possess native qualities.[68] For instance, in 2023-2024, authorities of several member States uncovered a large-scale disinformation campaign by foreign actors (the Doppelganger Operation), which systematically spread false content viewed a minimum of 850 000 times in the context of some key local, regional and national elections. In particular, in Germany, these fake posts touched upon the German support for Ukraine and were widely shared in the months leading to three key regional elections.[69] State authorities and social media platforms also faced challenges in accurately attributing responsibility for spreading false narratives and disinformation which impeded the

60 Commissioner for Human Rights, Council of Europe, Member states should enforce standards to combat online disinformation while protecting human rights for all, 10 January 2025
61 European Union External Action Service, "2nd Report on Foreign Information Manipulation and Interference Threats – A Framework for Networked Defense", January 2024.
62 Martin, D.A., Shapiro, J.N., Ilhardt, J.G., 'Online Political Influence Efforts Dataset, Version 4.0', 24 March, 2023,
63 Bennett, W. L., Livingston, S., eds., The Disinformation Age: Politics, Technology, and Disruptive Communication in the United States, 1st ed., Cambridge University Press, Cambridge, 2020, p. 171; Jung, H.M., 'Information Manipulation Through the Media', Journal of Media Economics, Vol. 22, No. 4, 30 November, 2009, pp. 188–210.
64 Bradshaw, S., Howard, P.N., Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation, Working Paper, Oxford, 2018,
65 Bradshaw, S., Bailey, H., Howard, P.N., University of Oxford, Industrialized Disinformation, 2020 Global Inventory of Organized Social Media Manipulation, 2020.
66 European Union External Action Service, "2nd Report on Foreign Information Manipulation and Interference Threats – A Framework for Networked Defense", January 2024; p11.
67 Targeted campaigns can exploit the vulnerabilities inherent to online social media, such as embedded biases or algorithmic functions, used to disseminate propaganda, amplify divisive narratives, and exploit emotional triggers. Starr, P., 'The Flooded Zone: How We Became More Vulnerable to Disinformation in the Digital Era', in Bennett, W.L., Livingston, S. (eds.), The Disinformation Age, 1st ed., Cambridge University Press, Cambridge, 2020, p. 80.
68 For example, including DeepL and ChatGPT. See Rumman Chowdhury, AI-fuelled election campaigns are here — where are the rules?, Nature, and "Election Disinformation in Different Languages is a Big Problem in the U.S.", Aliya Bhatia, Center for Democracy and Technology, 2022.
69 See for a full catalogue on the many ramifications of this disinformation campaign, "What is the Doppelganger operation? List of resources", EU Disinfo Lab, (last updated 30 October 2024).

implementation of effective countermeasures.[70] Many of these instances also involved a domestic component, as content has to be curated to a certain audience to reach its objectives. In the months leading up to the 2023 elections in Serbia, which were held simultaneously at local, provincial, and national levels, the Bureau for Social Research (BIRODI) called for legislative action regarding the suspected use of approximately 14 000 bots to manipulate public discourse on social media in favour of the ruling party.[71] In this context, some domestic stakeholders indicated the potential for foreign interference in the information environment as a significant concern.[72] Following the elections, the European Parliament urged Serbian authorities to address foreign interference and disinformation campaigns related[73] while Serbian President Vucić taxed other foreign actors of foreign interference and targeted the German members of international election missions without providing proofs.[74]

48. The undermining of electoral integrity, destabilising institutions and fostering of division through disinformation has also been very much feared in the context of regional identities and independence referendums. In 2020, a UK Parliament's intelligence and security committee investigation in potential Russian interferences in UK politics established that the 2014 Scottish independence referendum had been a target of disinformation tactics.[75] Notably, statements and videos on the vote being falsified were spread by foreign users and online accounts and viewed nearly a million times.[76] The UK Electoral Commission ruled that the elections had been organised in a fair and transparent manner but established that these baseless claims had an impact on the trust of voters in the results. Indeed, 42% of Scottish pro-independence voters believed that fraud took place, compared to 21% of "no" voters.[77] As mentioned above, in the context of the 2017 Catalonian independence referendum, bots were also involved in supporting the independentist option as well as foreign public broadcasters.[78] In addition, the French agency charged to tackle disinformation, Viginum, recently uncovered a targeted operation led by an Azerbaijani organisation to foster mistrust and division in New Caledonia, in a context of tensions related to the composition of the regional registers of voters. While it had limited success in exploiting independence movements and ideas, the agency still considered this organisation as a state propaganda outlet working against France, whose strategy is to instrumentalise public debate in overseas France to serve the objectives of Azerbaijan's foreign policy.[79] Such claims have been repeatedly voiced in the context of the Republika Srpska in Bosnia and Herzegovina[80] and ATU Gagauzia in the Republic of Moldova.

49. All actors accused of foreign interference have often strongly denied the allegations, while using the same rhetoric to put the blame on international observers, NGOs and foreign powers associated with democratisation projects namely Germany, the EU, the US, etc.

50. Smaller less-coordinated incidents related to the information environment have been witnessed in the context of local and regional elections throughout Europe, which show a modest but growing interest in these elections. For instance, in the 2021 municipal elections in Latvia, some false and misleading information on the elections was mostly shared by two news outlets associated with the Russian authorities.[81] In the 2020 local elections in Ukraine, several publications on local media were

70 An illustrative example is the assertion that implied a network of non-state entities, potentially linked to organised crime, orchestrated a cyber information manipulation campaign on behalf of the Russian government. The aim of the campaign was to sway British voters in favor of the United Kingdom's departure from the EU during the 2016 referendum. Intelligence and Security Committee of the UK Parliament, 'Russia', 21 July, 2020, p. 2,
71 See news articles in Serbian, e.g. 021, Analiza spiska 14.000 SNS botova: Evo koji gradovi u Srbiji su najveća bot-žarišta, 2023,
72 OSCE/ODIHR, Final Election Observation Report, 2024. *Op.cit.*
73 European Parliament, Joint motion for a resolution on the situation in Serbia following the elections, 2024,
74 Euractiv, Serbia president alleges foreign interference in elections, December 2023
75 BBC News, Sturgeon warns against 'complacency' over Russian interference, 21 July 2020.
76 In particular, Igor Borisov, an accredited observer from the Russian Federation labelled the referendum as "not meeting international standards" on Ria Novosti. Mr Borisov heads the Public Institute of Electoral Law, an organisation regularly involved in the organisation of biased election observation mission. See European Platform for Democratic Elections, International experts observing elections on the 2019 Russian single voting day and the Guardian, Russia cries foul over Scottish independence vote, September 2014.
77 See UK Electoral Commission Report on Scottish Independence Referendum, December 2014.
78 Erris Palmer, Spain Catalonia: Did Russian 'fake news' stir things up?, BBC News, September 2017.
79 See Technical report. Un-notorious BIG, a digital information manipulation campaign targeting French overseas departments, regions, territories and Corsica, Viginum, 2 December 2024.
80 See Wouter Zweers, Niels Drost & Baptiste Henry, Little substance, considerable impact Russian influence in Serbia, Bosnia and Herzegovina, and Montenegro, Cligendael, 2023.
81 Analysis of foreign influence and cyber incidents during the Latvian municipal elections 2021, DeBunkEU.Com for Sparta, 21 July 2021.

spotted by Media monitoring teams which reported Russian propaganda (in particular on troops in the Donbas), as well as some political contestants on social media.[82] One such case was also debunked which involved a fake communication between a party and the Security Service of Ukraine, in view of discrediting the latter.[83]

51. Another most recent example of large-scale foreign electoral interference including through information manipulation is the 2024 presidential election and constitutional referendum in the Republic of Moldova. According to the OSCE/ODIHR, the elections faced substantial concerns regarding illicit foreign influence and disinformation efforts primarily originating from the Russian Federation and home-grown political forces within the Republic of Moldova[84] that compromised electoral integrity, especially given the Republic of Moldova's insufficient legal framework to address such interference.[85] Such extensive information manipulation had already been noted in the context of the 2023 local elections in the Republic of Moldova. Indeed, research established that non-Romanian speaking minorities were more vulnerable to electoral disinformation, as they consumed mostly Russian-speaking media. In this context, and despite other available sanctions, the Commission for Exceptional Situations banned close to a dozen pro-Shor television channels, some of them among the most popular channels among non-Romanian speakers. These bans, also deplored by some NGOs and the Congress,[86] were easily circumvented and fed in disinformation on these channels as well as the narrative according to which the Moldovan government's decision constituting an unprecedented attack on the freedom of expression. Such drastic decision thus slightly backfired and was manipulated to feed in the mistrust in democratic processes.[87]

52. Likewise in the run up to the 2024 Georgian parliamentary elections, there have been direct attempts by Russia to interfere in elections especially through information manipulation. For instance, Russia's Foreign Intelligence Service (SVR) issued several statements accusing the United States of orchestrating a coup to unseat Georgian Dream.[88] Moreover, a network active on the social media platform Meta[89] targeted Georgian opposition that posted about protests against the foreign agent-law, inter-alia through fictitious news websites. In doing so, foreign actors aimed to blur the line between genuine political discourse and manipulated narratives, distorting public perception and complicating Georgians' ability to distinguish authentic public sentiment from foreign-influenced messaging.[90]

53. Another interesting trend is the involvement of transnational far-right groups in mobilising online and spreading disinformation. An example is the case of the 2018 State elections in Bavaria, Germany. In the last few years, regional elections in Germany have attracted international attention due to the rise of far-right parties and new voting patterns at local and regional levels (including in Thuringia and Brandenburg in 2024) in which far-right parties have gained position as kingmakers. A study of the Institute for Strategic Dialogue noted that "Both the international far-right and the Kremlin-sponsored media machine were active in the Bavarian case, each engaged in promoting communications in Germany to suit their own long-term agendas". Interestingly in the case of Bavaria, while Russian media outlets spread divisive speech and slightly favoured the AfD, no coordinated and systematic approach

82 See Council of Europe Website, How media cover the 2020 local elections in Ukraine – interim results of two monitoring activities, 8 October 2020.
83 See OPORA, Is Russia interfering in Ukrainian elections?, 19 October 2020,
84 Ibid., p. 2.
85 OSCE/ODIHR election observation report, presidential and parliamentary elections in Moldova, 2024, pp. 1-2.
86 In 2023, the Congress noted with concern "the enduring media concentration and the disinformation campaigns echoed on social media, contributed to unbalance an otherwise rather open media environment, in addition to the drastic decisions of the Commission for Exceptional Situations to ban dozens of media outlets due to national security concerns" and invited the authorities to "re-examine the wide-ranging powers granted to the Commission for Exceptional Situations and refrain from resorting to blanket bans of political parties and to the Commission for Exceptional Situations to restrict democratic freedoms during electoral campaigns". See Congress, Election Observation Report on the 2023 Local Elections in the Republic of Moldova, 2023, para. 11 and See Anticoruptie, "The People's Advocate requests additional arguments from CSE and SIS in relation to the suspension of the six TV stations", 31 October 2023
87 Matveyenko J., Assessing the Impact of Disinformation on Minority Communities in Moldova, December 2023.
88 Over the past few months, the SVR has released at least four statements alleging that the U.S. is staging a "Hollywood-style" plot to incite civil unrest and remove the ruling party through a so-called "Tbilisi Maidan"—a reference to Ukraine's 2013-14 uprising. The SVR further claimed that Russia seeks to prevent a "colour revolution" in Georgia by revealing its intelligence on the matter. See Atlantic Council, Russia is directly and indirectly meddling in Georgia's upcoming election, 2024,
89 In August 2024, Meta removed the network. Ibid.
90 Ibid. Russian intelligence has also engaged through assets on Georgian Telegram, including a channel dedicated to promoting the narrative of an imminent Western-organized "coup" around the elections. This channel is run by NewsFront, a Russian disinformation platform linked to Russian intelligence, which operates in multiple languages. Ibid. See also New Eastern Europe, Russian interference in Georgia's elections. How will the government respond?, 2024,.

to spread disinformation influence the elections was noted. The report however noted the importance of far-right transnational communities and their capacities to mobilise across borders to discredit journalists and opponents and promote mistrust and dissent. Such loosely connected networks can be more or less organised but often display a friendliness or allegiance to a foreign power and target the same aim to destabilise democratic institutions.

54. Concerningly, as many instances of foreign interference in electoral processes were raised by international observers, some member States have resorted to fake international observation to control the narrative on elections organised in their territories and to issue incorrect and biased reports. Therefore, representatives of local, national or international authorities have been invited to give credit to elections held with little regard for European electoral standards. German NGO coalition, the European Platform for Democratic Elections, has tracked the organisation of such missions and the identities of the so-called observers.[91]

### 3. Electoral cyberattacks

55. Electoral cyber-attacks can constitute another means of foreign interference, by targeting electoral infrastructure of all stakeholders involved in the process. New digital and cyber means allow for cyber-enabled interventions by hostile foreign actors in electoral processes. This applies even more since elections are particularly vulnerable to cyber risks due to their periodic nature and condensed timeframe with most activities centred around election day.[92] Electoral cyberattacks can include hacking voter registration databases, tampering with vote tabulation systems, spreading malware to disrupt voting machines, or the launching of distributed denial-of-service attacks to overwhelm election websites.[93] The threats listed below can impact election administration websites, but also political parties, candidates, government agencies, domestic observers and the media. [94]

56. However, it is important to mention that, despite the risk of large-scale impediments to the vote due to cyber-attacks, this fear has not materialised yet in local and regional elections in Europe. The Congress has only limited track record in observing e-voting or IT-powered counting systems (Finland, Georgia, Albania and Bosnia and Herzegovina) but has not witnessed large-scale cyberattacks linked to foreign powers on these systems so far. Lesser impact attacks have been recorded, but none seems to have compromised the orderly conduct of electoral processes. However, these attacks still consume resources granted to local and regional authorities, divert attention and place a heavy strain on electoral infrastructure.[95]

57. Due to the difficulty to investigate these cases, it is nearly impossible to attribute these attacks to either domestic or foreign agents, but most national security institutions currently attribute them to Russia, China and sometimes Iran.[96] In this context, the line between cybercrime and foreign interference is often blurred: indeed, some groups such as NoName057 promote resolutely foreign agendas but are difficult to clearly attribute to the national government.[97] Other campaigns such as Matrioshka and Ghostwriters have been uncovered and linked to a certain extent to foreign authorities.[98] Despite some highly mediatised cases in Europe, most examples have taken place outside the remits of the Council of Europe member States (US, Nigeria, Ghana, Philippines). However, it is important to

91 See the dedicated website of the European Platform for Democratic Elections at : https://epde.org/fake-observation/
92 Elections follow regular cycles that allow for extensive planning and preparation for attacks. Conversely, voting usually occurs within one day or over a few days, placing significant stress on the electoral system to manage a surge in activity and data within limited time. Van Der Staak, S., Wolf, P., Cybersecurity in Elections: Models of Interagency Collaboration, International Institute for Democracy and Electoral Assistance, 2019, p.19,.
93 Despite the misconception that only highly digitalised countries are vulnerable to cyberattacks, most elections worldwide rely to some extent on ICT tools. See the examples below. Moreover, Attributing cyberattacks is a complex and sensitive process, as attackers often employ sophisticated techniques to conceal their origins and possible motives. See below the example of cyberattacks that occurred in the German federal elections.
94 Cyber threats related to elections may also encompass cyber espionage aimed at gathering information about the political positions of candidates and political parties. This acquired information can then be leveraged for subsequent operations, such as conducting disinformation campaigns. McNamara, L., 'Framing the Problem: Cyber Threats and Elections', Mandiant, 2019,
95 For example, see Reuters, 'Czech Election Websites Hacked, Vote Unaffected - Statistics Office', 22 October, 2017,
96 Where do cyber threats come from?, Centre d'Etudes Européennes, Sciences Po, April 2024. and Bruce M, Lusthaus J, Kashyap R, Phair N, Varese F (2024) Mapping the global geography of cybercrime with the World Cybercrime Index.
97 Declan Carey, Pro-Russia hackers claim council cyber attacks, BBC News, 31 October 2024.
98 To learn more about these campaigns, see MATRYOSHKA, A pro-Russian campaign targeting media and the fact-checking community, Viginum (France), 2024 and the Ghostwriter campaign as as a multivector information operation, Cardiff University, Security, Crime and Intelligence Innovation Institute (2023).

note that these cases have built knowledge and experience among the cyber security community and the threat does not seem to be as high as perceived a few years back and election management bodies are less immune to these attacks at national levels.[99] It is unclear however how lower levels of election management bodies fare when confronted with such threats.

58. More common but lesser impact attacks are DoS and DDoS. A Denial-of-Service (DoS) attack uses a single computer to flood a target with traffic and are easier to block, while a Distributed Denial-of-Service (DDoS) attack involves multiple compromised devices (a botnet) sending traffic simultaneously. DDoS attacks are harder to defend against and can disrupt critical election services like voter registration databases, online voting systems, or election information portals.[100] Many election administration websites have suffered from DoS/DDoS attacks, mostly in the context of national elections (Montenegro 2016, Czechia 2017, North Macedonia 2020[101]). However, some cases have related to local and regional elections. In the 2014 Slovak local elections, interim results were presented on the website of the Statistical Office, as well as on a parallel contracted secured website. Three waves of hacker DDoS attacks were held nearly simultaneously and but were resolved quickly and results were published in a timely manner on the other website. In the context of the 2015 local elections in Bulgaria (and referendum on e-voting), the Central Election Commission of Bulgaria and several ministries were exposed to a massive DDoS attack on election day. In particular, the CEC's website received attempts by 65 000 000 users to access the website at the same time. In total that day, 530 000 000 connections were made, and a quarter of these visits originated from Vietnam, Türkiye, and US-based IP addresses.[102] The President of Bulgaria later attributed the attack to foreign actors (APT28).[103] Early October 2024, only a few days before the Belgian communal elections, several websites of local authorities were targeted by DDoS over the course of five days, allegedly originating from foreign hackers based in Russia, but with limited consequences other than impossibility to access these websites for few minutes.[104] The same type of relatively unsuccessful attacks took place just before the election day in Ireland (both European and local elections) and impacted voter.ie, the official website to check voter registration.[105]

59. Another type of cyberattack concerns website defacement. It involves altering a website's appearance and content and is not limited to election administration websites. It can also target various actors within the electoral ecosystem, including political parties, candidates, government agencies, and organisations involved in election monitoring and transparency. Additionally, media outlets and social media platforms have been subject to website defacement attacks.[106] For instance, Russia initiated a cyberattack against the website of the Polish electoral commission in 2014, seeking to undermine the credibility of the local elections.[107] In the same year, the network of the Ukrainian Central Election Commission was targeted for defacement and exploitation by Russian military hackers.[108] In the context of the 2024 local elections in Bosnia and Herzegovina, the IT unit of the Central Election Commission also realised that a fake CEC website had been established which was quickly taken down.[109]

60. Another common online threat is the disruption or interception of communication via (spear)phishing (sending fraudulent emails as if from a reputable source), malware (a software intentionally designed to cause disruption to a computer) and ransomware (a malware denying access to a computer's data). In 2024, the UK National Cyber Security Centre identified ransomware as the biggest cyber threat facing the UK that year, the year of local elections (and early parliamentary

99 Kosak M., Cybersecurity & the 2024 US Elections, September 2024.
100 Van Der Staak, S., Wolf, P., Cybersecurity in Elections: Models of Interagency Collaboration, International Institute for Democracy and Electoral Assistance, 2019,
101 Oliver Risteski, Intrusions on State Digital Infrastructure in North Macedonia: Digital Human Rights Impact Analysis, DCAF Young Faces Participant 2022
102 Huge Hack Attack on Bulgaria Election Authorities 'Not to Affect Vote Count', Novinite, 27 October 2015,
103 Gordon Corera, Bulgaria warns of Russian attempts to divide Europe, BBC News, 4 November 2016.
104 RTBF, « Cyberattaques de sites d'autorités belges : "L'objectif est de décrédibiliser les autorités à quelques jours des élections" », 8 October 2024 (in French).
105 Government websites hit with cyber attack day before elections, pro-Russian hackers suspected, The Journal, 8 June 2024.
106 For instance, on 6 May 2018, during Latvia's general election, the social network Draugiem was targeted for website defacement. The defaced page displayed a pro-Russian message stating, "Comrades, Latvians, this concerns you. The borders of Russia have no end," accompanied by images of Russian soldiers in Crimea and military parades in Moscow. Public Broadcasting of Latvia, 'Draugiem.Lv Social Network Hacked with pro-Russia Message', 6 October, 2018,
107 AP News, 'Polish Election Commission Website Hacked', 19 November, 2014,
108 The Atlantic Council, 'Foreign Interference in Ukraine's Democracy', 15 May, 2019,
109 Congress 2024 election observation mission to Bosnia and Herzegovina.

elections). The report stated that in 2022 the UK was the second most ransomware-attacked country globally after the US and most attacks originated from foreign perpetrators.

61. Other cases of malicious cyber activities during local elections include,[110] for instance, the U.S. democratic primaries in July 2018 where two local democratic campaigns experienced DDoS attacks, disrupting online fundraising efforts by hampering access to donation platforms and campaign websites.[111] Infrastructure supporting elections, such as voter registers, electoral commissions, and electoral boards, represent another category of targets.[112] In 2023, the UK Election Commission revealed that the voter registers were hacked for over a year (between August 2021 to October 2022) and personal information held on the Electoral Register had been compromised, due to the lack of protection of its IT systems.[113] The UK government latter blame the attack on Chinese operatives.[114] In August 2022, a few weeks before key local elections, Montenegro suffered a large scale cyber-attack, attributed to "Cuba ransomware", which curtailed the functioning of many governmental agencies for close to 20 days. Montenegro's Agency for National Security blamed Russia, but others pointed at criminal gangs operating within the umbrella of Russian influence. While attacks directly aimed at weakening the core electoral infrastructure, including vote tabulation systems or voting machines, pose the greatest risk, there is limited evidence of intrusion activity targeting this critical infrastructure in local elections.[115]

62. An illustrative case of electoral cyberattacks occurred during Germany's federal elections. Prior to the 2015 federal elections, the computer system of the German *Bundestag* was targeted in a cyber assault attributed to Russia.[116] This attack aimed to gather intelligence for potential use in disinformation campaigns or influence operations.[117] Additionally, the perpetrators attempted to steal email credentials from members of the Christian Democratic Union of Germany (CDU).[118] Furthermore, ahead of the 2021 German federal elections, a DDoS attack disrupted the website of the Federal Returning Officer, responsible for overseeing federal-level elections. Consequently, the website was temporarily unavailable. Concurrently, in the months leading up to the elections, a group known as 'Ghostwriter', linked to the Russian GRU military intelligence service, launched a hacking campaign against German federal and state MPs.[119] The hackers sent phishing emails to steal personal login data from German lawmakers. Although Germany publicly attributed the illegal cyber activities of 'Ghostwriter' to Moscow, it was later also argued that Belarus was at least partially responsible for the group's activity.[120] Significantly, while it remains uncertain whether the malicious cyber activities aimed at the 2021 German elections were coordinated, this case underscores that hostile actors may employ a combination of techniques targeting various levels of the electoral ecosystem.

63. While it may be unlikely that the election outcome be changed by these attacks,[121] successful cyber-attacks can erode public confidence, hinder voter participation, and potentially disenfranchise eligible voters. Cumulatively, cyberattacks, each with limited material impact individually, can have multiplied psychological effects, creating an illusion that the entire election process was compromised.[122]

110 McNamara, L., 'Framing the Problem: Cyber Threats and Elections', Mandiant, 30 May 2019,
111 Bing, C., 'Two Democratic Campaigns Hit with DDoS Attacks in Recent Months', CyberScoop, 9 July 2018,.
112 Lim, Y., 'Election Cyber Threats in the Asia-Pacific Region', Mandiant, 22 November 2020,
113 UK Information Commissioner's Office, ICO reprimands the Electoral Commission after cyber attack compromises servers, 30 July 2024
114 Soraya Harding, China's UK election hack – how and why the Electoral Commission was targeted, University of Portsmouth Blog, 27 March 2024.
115 McNamara, L., 'Framing the Problem: Cyber Threats and Elections', Mandiant, 30 May, 2019, h.
116 Deutsche Welle, 'Bundestag IT System Shut Down', 20 August, 2015,
117 Committee on Foreign Relations, U.S. Senate, 'Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security', A Minority Staff Report, 10 January, 2018,
118 Auchard, E., 'Hackers Try to Attack Merkel's Party, Security Consultants Say', Reuters, 11 May, 2016,
119 Page, C., 'EU Warns Russia over "Ghostwriter" Hacking Ahead of German Elections', TechCrunch, 24 September, 2021,
120 Mandiant, 'UNC1151 Assessed to Have Links to Belarusian Government', 16 November, 2021,
121 Delerue, F., Cyber Operations and International Law, Cambridge Studies in International and Comparative Law, Cambridge University Press, Cambridge, p. 255, 2020.
122 The European Union Agency for Cybersecurity, ENISA Threat Landscape 2022,

## IV. FOREIGN INTERFERENCE: A THREAT TO SOVEREIGNTY, DEMOCRATIC SELF-DETERMINATION AND HUMAN RIGHTS EUROPEAN AND INTERNATIONAL OBLIGATIONS

### 1. A grey area of international law

64. Foreign electoral interference raises significant challenges under international law, particularly concerning state sovereignty, democratic self-determination, and human rights obligations. Sovereignty entails the right of states to exercise exclusive control over their territory and functions, and violations occur when foreign interference undermines territorial integrity, governmental operations, or election infrastructure. Similarly, the principle of non-intervention[123] prohibits coercive interference in a state's domestic affairs, including electoral systems. While actions like cyberattacks causing lasting harm to election processes are generally regarded as breaches of sovereignty,[124] more subtle actions, such as misinformation campaigns, often require nuanced, case-specific assessments to determine their coercive nature.[125]

65. These issues are equally relevant at national and local levels, where foreign interference may distort democratic self-determination and undermine local governance rights. Foreign interference may encroach upon the democratic self-determination[126] of a particular society or group, by distorting the balance within this group, in particular through mis- or disinformation or funding at local or regional levels.[127] Respectively, the Charter establishes in Art. 3(2) that the right to local self-government "shall be exercised by councils or assemblies composed of members freely elected by secret ballot on the basis of direct, equal, universal suffrage". This may be put in question in instances of foreign electoral interference with negative impacts on local democracy.

66. Furthermore, the interfering state's extraterritorial human rights obligations add complexity. Foreign interference can jeopardise rights related to fair elections, free expression, and privacy, emphasising the need to hold interfering states accountable. Election interference by a foreign state is inherently extraterritorial[128] and relies on the assumption that the interfering state has the obligation not to violate the human rights of the individuals/population on another state's territory but is hardly applicable. Furthermore, the attribution of such interference to a specific state is often challenging due to the indirect involvement of private actors or the difficulty of tracing cyber activities. Rules on state responsibility, including effective control over non-state actors, guide attribution but leave many cases unresolved.[129]

---

123 See Art. 2(1) United Nations Charter, sovereign equality of states. Its applicability to foreign interference (especially with regard to cyber space) has been repeatedly confirmed. According to customary law, intervention is defined by two key elements: both of which must be met to constitute a breach of international law: Firstly, a foreign interference must impact the internal or external affairs of another state, known as its "*domaine réservé*". Electoral systems typically fall within the *domaine réservé*. Secondly, the interference must be "coercive in nature". The two elements were outlined by the International Criminal Court (ICJ) in para. 205 of the Nicaragua judgment. Nicaragua v. United States, Judgment on Jurisdiction and Admissibility, ICJ GL No 70, [1984] ICJ Rep 392, ICGJ 111 (ICJ 1984), 26th November 1984, United Nations [UN]; International Court of Justice [ICJ]. The "domaine réservé" constitutes the field of activity left by international law to states to regulate, states enjoy discretion to make their own choices, as explicitly exemplified by the ICJ in the case of elections. Elections represent a paradigmatic example of a matter that is encompassed in the domaine réservé; in fact, the ICJ cited the "choice of political system" to illustrate the concept. As explained by the ICJ in the Nicaragua case "The element of coercion… defines, and indeed forms the very essence of, prohibited intervention."

124 Schmitt, Foreign Cyber Interference in Elections: An International Law Primer, EJIL, Articles I-III,

125 Several states have indeed considered especially cyberattacks by foreign actors as violation of the sovereignty rule. For example, France, the Netherlands, Germany, Iran, the Czech Republic, Austria, and Switzerland (not the UK, however) consider foreign electoral interference in form of cyberattacks as breach of national sovereignty. It appears NATO is also inclining towards this perspective.

126 See the right to self-determination e.g. in Arts. 1 ICCPR, ICESCR; Art. 1(2) UN Charter.

127 See in this sense Uerpmann-Wittzack: „Those who support an organisation [CB: political parties] with important funds may do so in order to implement their own agenda and to give particular weight to their own goals. A democratic society by contrast is based on the principle of democratic equality of all citizens. Therefore neither economic power nor external actors should bias elections and public debate." Robert Uerpmann-Wittzack, Freedom of Association: The Shrinking Space of Civil Society, Tutzing, September 2020,

128 Schmitt, Foreign Cyber Interference in Elections: An International Law Primer, Part II, EJIL,

129 Relevant rules are incorporated in the International Law Commission's (ILC) 2001 Articles on the Responsibility of States for Internationally Wrongful Acts (Articles on State Responsibility). In principle, a state may be responsible for violations of international law by state organs (Art. 4). Moreover, also the acts of private actors (e.g. hackers) may be attributable to a state, inter alia in cases where the state exercises effective control (Art. 8) or adopts their conduct as its own (Art. 11). Therewith, acts of foreign electoral interference need to be either directly pursued by state organs or (more frequently) the state must exercise control of the relevant private actors which interfere.

## 2. International Human Rights Obligations

67. In light of the potentially severe consequences outlined above, states may indeed be justified (or even obliged) to take positive action to prevent and/or counter such interferences with electoral processes, in general and especially from foreign actors. At the same time, also the very measures pushing back on foreign interference may impact upon/interfere with human rights, e.g. imply restrictions of the right to freedom of expression when certain content is suppressed. Indeed, some of these attempts to interfere by foreign actors clearly cross existing legal thresholds (illegal funding, hate speech), some sit in a grey zone of acceptability in many member States (misleading information, microtargeting, etc).

68. This is exemplified by the controversies surrounding the recent adoption of foreign agents' laws which prohibits, limits or unduly regulates funding from foreign sources to NGOs in various countries, such as Russia, Georgia, Hungary and also the EU.[130] The according laws/prohibition of foreign funding show the tension between undue restriction of freedom of association and a due protection against foreign interference. Although such laws may not always aim to the prohibition of NGOs funded by external actors, they may stigmatise them in the eyes of the public and make them vulnerable to further limitations imposed by the state and ultimately stifle free speech.[131]

69. A human rights perspective on state measures will have to calibrate between the obligation to protect (the integrity of elections, the free expression of the will of voters) and the obligation to respect human rights (the freedoms of expression, association etc.) by a state which takes action against foreign electoral interference. Several human right standards including the right to free elections/political participation and the adjacent freedoms of expression and (assembly and) association establish the main regulatory framework for relevant state action to counter foreign interference in electoral processes. They provide the basis for elections to be held in accordance with international standards, allowing for "genuine" elections and the free expression of the will of voters in local and regional elections.

70. The ECtHR's "justification test" assesses the permissibility of restricting human rights to counter foreign electoral interference, requiring any measure to be lawful, to pursue a legitimate aim, to be "necessary in a democratic society", i.e. be proportional.[132] To uphold electoral integrity and/or a level playing field between candidates when coping with foreign electoral interference, a state may thus justify according restrictions of the freedom of expression (e.g. to contain information manipulation) or freedom of association (e.g. to prevent foreign funding of political parties) under condition that they are clear, not arbitrary and do not unlawfully discriminate against a particular group, , with criteria varying depending on the rights affected.[133]

### 2.a. Right to political participation

71. As mentioned above, the primary right at stake in case of foreign electoral interference is the right to political participation (as provided for in Art. 25 ICCPR and Art. 3 of Protocol 1 of the ECHR). Both contain roughly similar guarantees which may be put to detriment in case of foreign interference. Under the ECHR, the right to free elections[134] establishes that states parties "undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature".[135] This includes the right to vote and to

130 Human Rights Watch, Foreign Agent Laws in the Authoritarian Playbook, 19 September 2024,
131 See Venice Commission Opinion 1190/2024 on Georgia "Urgent Opinion on the Law of Georgia on Transparency of Foreign Influence", adopted in June 2024 and 1169/2023 on Hungary "Opinion on Act LXXXVIII of 2023 on the Protection of National Sovereignty", adopted in 2023.
132 See the respective paras. 2 of Arts. 10 and 11 ECHR; see for details Council of Europe, Guide on Article 10 of the European Convention on Human Rights, Part III; And Council of Europe, Guide on Article 11 of the European Convention on Human Rights, Part D.
133 There need to be safeguards in place against arbitrariness – e.g. ex ante control; ongoing accompaniment of measures; ex post control by independent institutions.
134 Note however, that only elections for legislative bodies are protected by the ECHR which excludes most local elections and a significant part of regional elections (ECtHR, *Py v. France*, no. 66289/01). Nonetheless, the ECtHR has found admissible cases of local and regional elections where other rights were violated, e.g. Art. 10 (right to freedom of expression, ECtHR, *Şükran Aydın and Others v. Turkey*, no. 14871/09, 22 January 2013.
135 In order to effectively guarantee/implement the right to free elections, certain electoral principles and conditions must be complied with. Firstly, the principles of *universal, equal, free, secret and direct suffrage* are key to realise the right to political

stand for elections. It also entails a state's positive obligation to provide for conditions under which people can freely form and express their opinions and choose their representatives.[136] The Charter also establishes in Art. 3.2 that the right to local self-government "shall be exercised by councils or assemblies composed of members freely elected by secret ballot on the basis of direct, equal, universal suffrage."

### 2.b. Freedom of expression

72. Freedom of expression is intrinsically linked to the right to free elections/electoral integrity.[137] This is affirmed by the ECtHR and also by the Venice Commission. Respectively, the Court considered both as crucial to establishing and maintaining the foundations of an effective and meaningful democracy governed by the rule of law.[138] The Venice Commission held that "[t]he right to free elections […] also entails a positive obligation on the member states to ensure conditions under which people can freely form and express their opinions and choose their representatives. […] the rights to freedom of expression and to free elections are prerequisites of each other."[139] As held by the ECtHR, it is particularly important for the period preceding an election that opinions and information of all kinds are permitted to circulate freely.[140]

73. Freedom of expression (Art. 10 ECHR), includes "the freedom to hold opinions and to receive and impart information and ideas without interference by public authority." Art. 10 ECHR not only protects the content of information but also the methods of its dissemination, as any limitation based on the latter inevitably infringes upon the right in both dimensions, i.e. to receive and impart information.[141] Therefore, Art. 10 ECHR's scope of application is broad and comprises rights in the digital sphere, including on social media.[142] In fact, the ECtHR made clear that online media and bloggers are likewise protected under Art. 10 ECHR. [143] The Court has also recognised individuals' right to access the internet. [144]

74. At the same time, a state may, to safeguard electoral integrity, see itself forced to restrict the freedom of expression of contestants, voters or other electoral stakeholders, including foreign agents.[145] This is recognised by the ECtHR regarding the right to freedom of expression in the context of election

participation. Universal suffrage entails that everyone has the right to vote and to stand for election, based on reliable electoral registers and subject to certain conditions. Equal suffrage requires that each voter have one vote and equal voting power within electoral constituencies, as well as that candidates and parties have equal opportunities in elections. Free suffrage means that voters are free to form an opinion but also that they have freedom to express their wishes and action to combat electoral fraud. Secret suffrage protects a voter's privacy. All these standards may be at stake in case of foreign electoral interference

136 See *Communist Party of Russia and Others v. Russia,* App no 29400/05 (ECtHR, 19 June 2012), paras. 51, 79, 108, 126.

137 C.f. Joint Report of the Venice Commission and of the Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI), on Digital Technologies and Elections, Venice Commission CDL-AD(2019)016. Right to free elections, as incorporated in Art. 3 P 1, effectively promotes "true democracy".

138 ECtHR, *Orlovskaya Iskra v. Russia*, para. 10; see also ECtHR, *Hirst v. the United Kingdom (no. 2)* [GC], para. 58.

139 See the Venice Commission (CDL-AD(2019)016, para. 50; 51.

140 Ibid; See also *Orlovskaya Iskra v. Russia (*2017). According to the ECtHR, the role of the media during election time encompasses an independent exercise of freedom of the press on the basis of free editorial choices aimed at imparting information and ideas on subjects of public interest, thus strengthening voters' ability to make informed choices at the polls. (para. 130).

141 *Autronic AG v. Switzerland* App no 12726/87 (ECtHR, 22 May 1990).

142 In the digital public sphere, content policies must adhere to the principles of freedom of expression. Ensuring an open public debate is pivotal in this regard: the ECtHR indeed highlighted the significance of "the free exchange of opinions and ideas", which is essential for fostering a democratic environment. *Gillberg v. Sweden* App no 41723/06 (ECtHR, 3 April 2012).

143 *Observer and Guardian v. the United Kingdom* App no 13585/88 (ECtHR, 26 November 1991); *Guerra and Others v. Italy* App no 116/1996/735/932 (ECtHR, 19 February 1998).

144 The ECtHR asserted that "the internet has now become one of the principal means of exercising the right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest". Blocking the access to the internet was thus found in violation of Art. 10 ECHR when the measure in question produced arbitrary effects and the judicial review of the blocking of access had been insufficient to prevent abuses. *Ahmet Yıldırım v. Turkey* App no 3111/10 (ECtHR, 18 December 2012).

145 C.f. Venice Commission Joint Report 2020, para. 44: „For example, according to ECtHR, the rights to freedom of expression and to free elections are on the one hand prerequisites of each other, but on the other hand they may conflict and it may be considered necessary, in the period preceding or during an election, to place certain restrictions on freedom of expression, of a type which would not usually be acceptable, in order to secure the "free expression of the opinion of the people in the choice of the legislature".

campaigns,[146] where the Court emphasised that the phrase in Art. 3 of Protocol 1 providing for "conditions which will ensure the free expression of the opinion of the people in the choice of the legislature" implies not only the freedom of expression but also the principle of equal treatment of all citizens in exercising their right to vote and to stand for election.[147] Accordingly, the ECtHR emphasised the state's responsibility to prevent inequality in media coverage during elections (both in online and offline contexts).[148] Therefore, in certain circumstances, restrictions of the freedom of expression may be justified or even warranted in electoral processes, to ensure the "free expression of the opinion of the people in the choice of the legislature". The ECtHR also generally acknowledges that in balancing the freedom of expression versus the integrity of elections, states have a margin of appreciation which varies with the circumstances of the case.[149]

75. In extreme cases, such as hate speech or foreign electoral interference involving defamation of entire groups, states may be obliged to restrict freedom of expression to fulfil their duty to protect, as per Art. 20 ICCPR[150] and Art. 17 ECHR.[151] Restrictions may also be necessary to safeguard others' rights under Arts. 8 and 14 ECHR, as seen in cases like *Beizaras and Levickas v. Lithuania* (2020),[152] where inadequate state action against hate comments violated anti-discrimination and privacy rights. Similarly, failure to remove harmful online content can lead to state liability, as in *K.U. v. Finland*. [153] States are thus obligated to restrict speech, including hate speech used in foreign electoral interference, to protect others.

76. In less severe cases, states may justify restricting the freedom of expression, particularly to counter electoral disinformation, if evaluated by the ECtHR through a "justification test" requiring lawfulness, legitimate aim, and necessity, to avoid a potentially chilling effect of restrictions on the media. Especially in the context of electoral disinformation**,** there are indeed limits to the freedom of expression**.**[154] The Court distinguishes between facts and opinions/value judgments, affording stronger protection to opinions while allowing stricter measures against false factual assertions. [155] The ECtHR has pointed out that opinions are less "susceptible of proof," and must therefore be protected more robustly than false assertions of facts. At the same time, the ECtHR emphasised the importance of the medium used to spread disinformation. Notably the internet's vast, persistent[156] and rapid reach heightens the potential harm of disinformation in comparison to the traditional media, [157] justifying more extensive restrictions based on the scope of its public impact.[158]

77. Moreover, states have significant leeway to curb disinformation in paid political advertisements to prevent undue foreign financial influence and uphold media pluralism. The Court has recognised the

146 Freedom of political debate form the foundation of any democracy. Therefore, it is particularly important in the period preceding an election that opinions and information of all kinds are permitted to circulate freely (*Orlovskaya Iskra v. Russia*, para. 110).
147 ECtHR, *Mathieu-Mohin and Clerfayt v. Belgium*, para. 54.
148 *Communist Party of Russia and Others v. Russia* App no 29400/05 (ECtHR, 19 June 2012).
149 ECtHR, *Animal Defenders International v. the United Kingdom* [GC], para. 123; ECtHR, *Oran v. Turkey*, para. 52; ECtHR, *Bowman v. the United Kingdom* [GC], para. 43.
150 Art. 20 ICCPR: "…2. Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."
151 The limits of freedom of expression in case of defamatory and hate speech are also reflected when the ECtHR applies the "abuse clause", which implies that the respective instances of hate/defamatory speech are outside the scope of the ECHR. in cases where Art. 17 has been invoked, the refusal of the ECtHR to apply Art. 10 has meant that the Court has not examined interferences under its traditionally useful three-pronged test. Hannie and Voorhoof, Netherlands Quarterly of Human Rights, Vol. 29/1, 54–83, 2011.
152 ECtHR, *Beizaras and Levickas v. Lithuania,* 14 January 2020. The applicants, two young men who were in a relationship, alleged that they had been discriminated against on the grounds of sexual orientation because of the authorities' refusal to launch a pre-trial investigation into the hate comments on the Facebook page of one of them. The Court held that there had been a violation of Art. 14 taken in conjunction with Art. 8, finding that the applicants had suffered discrimination.
153 See ECtHR, *K.U. v. Finland*, 2008.
154 Note however, that regarding disinformation that does not involve elements of hate speech, it is noteworthy that nothing in Art. 10 ECHR requires citizens to impart 'truthful information' and thus the fact that statements may mislead (deceive) citizens does not necessarily mean that they should be restricted. Tarlach McGonagle (2020) Defamation law reform, the European Convention on Human Rights and EU law,
155 This distinction is important when considering electoral disinformation because it fits neatly with academic distinctions between disinformation and misinformation, i.e. disinformation involves knowingly false information while misinformation is merely be shared out of mistake and without malicious intent. ECtHR, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary,* paras. 60 et seq.; ECtHR*, Delfi AS v. Estonia* [GC], paras. 142 et seq Shattock 2022, pp. 6-7).
156 ECtHR, *Delfi AS v. Estonia* [GC], para. 110.
157 ECtHR, *Féret v. Belgium*, para. 76.
158 ECtHR, *Savva Terentyev v. Russia*, para. 79; ECtHR, *Delfi AS v. Estonia* [GC], para. 133; See more on different categories of unlawful speech in the Council of Europe, Guide on Article 10, 2.a.-2.c., pp. 96-99.

risk of competitive advantages gained by powerful financial means which can result in undermining the fundamental role of freedom of expression in a democratic society.[159] Media pluralism is especially at risk due to the usage of larger resources when the impugned advertisements are political in nature,[160] with a state thus enjoying discretion to establish according restrictions. [161] Indeed, the Court has noted that there is no European consensus on how to regulate paid political advertising in broadcasting[162] which broadens the margin of appreciation to be accorded to the State as regards such restrictions on public interest expression, including from foreign sources.[163]

### 2.c. Freedom of Assembly and Association

78. Freedom of assembly and association are essential preconditions for free and fair elections and safeguards for the formation of political movements, including the establishment of political parties and the possible formation of democratic will.[164] The freedom of (assembly and) association (Art. 11 ECHR) [165] is therefore particularly relevant when analysing foreign funding of political parties, especially as regards the permissibility of restrictions concerning the foreign funding of political parties.

79. The ECtHR has developed criteria for justifiable restrictions on political parties, particularly when their manifestos conflict with democratic principles.[166] Such restrictions must be lawful, pursue legitimate aims, and be "necessary in a democratic society", i.e. be proportional,[167] with extreme measures like party dissolution only permissible when absolutely necessary. State regulations must uphold non-discrimination and equal treatment, ensuring no group or individual is unfairly targeted or advantaged and must develop in detail what is unlawful and what are the related permissible sanctions. [168] Equal treatment under the law is imperative, preventing any undue advantage or disadvantage in the formation and operation of political parties. While financial oversight of political parties is essential for transparency and accountability, the ECtHR stresses that these measures must not become tools for political control in order to maintain public trust in elections, requiring high foreseeability in laws governing financial inspections and sanctions. [169]

80. Political party and campaign finances, including how to deal with foreign donations, is indeed critical to deal with foreign electoral interference through the funding of political parties, candidates, and referendum campaigns. A state's *margin of appreciation* to restrict such foreign funding activities is rather broad. Even prohibiting political parties from receiving funds from foreign sources is not in itself incompatible with Art. 11 ECHR. States generally remain free to determine which sources of foreign funding may be received by political parties under condition that the ban is not arbitrary. Indeed, the

159 See ECtHR, *Verein gegen Tierfabriken v. Switzerland*, para. 73.
160 ECtHR *Murphy v. Ireland*, para. 74; ECtHR, *Animal Defenders International v. the United Kingdom* [GC]. In the *Animal Rights Defenders v. UK* case, the ECtHR explicitly recognised the potential of powerful political groups to gain competitive advantages and did not find a violation accordingly.
161 Good faith in spreading misinformation, a key consideration for the ECtHR, is less relevant in cases of foreign electoral interference, as such acts are typically malicious. However, in ***Brzeziński v. Poland*** (2019), the Court found a violation of Article 10 because Polish authorities failed to differentiate between deliberate falsehoods and good faith criticism when addressing allegations made by an election candidate, emphasizing the need for careful evaluation in restricting freedom of expression.
162 ECtHR, *Animal Defenders International v. the United Kingdom* [GC], para. 123.
163 Ibid., para. 123; ECtHR, *TV Vest AS & Rogaland Pensjonistparti v. Norway*, para. 67; ECtHR, *Société de conception de presse et d'édition and Ponson v. France*, paras. 57 and 63.
164 Venice Commission Code of Good Practice in Electoral Matters, Explanatory Memorandum, 2002, p. 33.
165 Venice Commission Code of Good Practice in Electoral Matters, 2002. See ECtHR, *United Communist Party of Turkey and Others v. Turkey,* application no. 19392/92, 30 January 1998. Political parties have an important role in a democratic society. The ECtHR has noted that political parties are a form of association essential to the proper functioning of democracy.
166 ECtHR, *Refah Partisi (the Welfare Party) and Others v. Turkey* [GC], 2003; ECtHR, *Linkov v. the Czech Republic,* 2006.
167 Venice Commission, Code of Good Practice in Electoral Matters, Explanatory Memorandum, 2002, p. 33. Although the Court has never ruled on cases regarding campaign finance regulations in the context of restrictions of Art. 3 of Protocol 1, it can be deduced from its case law that such restrictions would be evaluated through two criteria: whether there has been arbitrariness or a lack of proportionality, and whether the restriction has interfered with the free expression of the opinion of the people. In addition, the Court has underlined the need to assess any electoral legislation in the light of the political evolution of the country concerned. Also, stricter requirements may be imposed on eligibility to stand for election than is the case for eligibility to vote. Paras 11-15 of the Council of Europe, Guide on Article 3 of Protocol 1.
168OSCE/ODIHR and Venice Commission Guidelines on Political Party Regulation have detailed the criteria for permissible restrictions and limitations of the right to freedom of association: According to the OSCE/ODIHR Guidelines, legally imposed limitations should find their basis in the state's constitution or parliamentary acts which define in detail what activities are deemed unlawful and what are the corresponding sanctions in case of violations. Principles 1-10 of the Venice Commission Guidelines and Report on the Financing of Political Parties, 2001.
169 Given the pivotal role political parties play in the effective functioning of democracies, it can be argued that the general public has a vested interest in their monitoring and the enforcement of penalties for any irregular spending. ECtHR, *Cumhuriyet Halk Partisi v. Turkey,* 2016, para. 69.

prohibition on the funding of political parties by foreign States may be necessary for the preservation of national sovereignty.[170] Foreign financing is considered problematic[171] and may in principle be legitimately banned also in the framework of the ECHR.

81. As regards the permissibility of state measures interfering with the respective rights, there may indeed be a distinction between freedom of expression and freedom of association as regards foreign funding, e.g. of political parties. Especially the latter may be considered as more disruptive to the electoral process and endangering national sovereignty/democratic self-determination at all levels of government. [172]

82. Moreover, further rights are indirectly of relevance for elections in accordance with international standards. The prohibition of discrimination (Art. 14 of ECHR and Art. 1 of Protocol No. 12) requires equal treatment of all and prevents arbitrary differentiations between individuals. The provision has been applied by the ECtHR concerning various cases of restrictions of the right to vote and to be elected in elections (including at local level), as well as of the freedoms of expression, assembly and association in the electoral context.[173] The rights to fair trial and an effective remedy (Arts. 6, 13 ECHR) in case of alleged violations of (electoral) rights presuppose review by independent and impartial courts and are thus essential institutional guarantees. Furthermore, and of particular significance in the digital sphere, is the right to private life (Art. 8 ECHR): Indeed, in its jurisprudence, the ECtHR has developed detailed standards for the protection of personal data[174] which is of relevance for the protection of privacy rights in electoral processes too.

## V. STANDARDS AND BEST PRACTICES TO PREVENT, DETECT AND COUNTER FOREIGN INTERFERENCES IN LOCAL AND REGIONAL ELECTORAL PROCESSES

83. While there is no one solution to handle interferences, public resilience and awareness of the threats and challenges constitutes the best protection currently available, as actors can take various ways to interfere with elections. Transparency and evidence are needed to ensure the public can detect and understand the motives of such actions. Therefore, general awareness of voters and candidates/political parties is key to ensure reactivity to it. While such awareness exists to a certain extent for national elections, it does not easily translate to local self-government levels. A French Senate Report, taking stock of the lack of awareness of elected representations, recommended systematically convening municipal, département and regional elected representatives and local security services after the elections to discuss foreign interferences.[175]

84. Since 2015, the EU has also been very proactive in helping states build their capacities and cooperate more systematically (via exchange of information and task forces) on the topic of foreign interferences, by developing a dedicated committee, the Special committee on foreign interference in all democratic processes in the European Union, including disinformation (ING2) and various strategies, studies and recommendations.[176] The European Union External Action unit also developed a tool box and framework to address foreign information manipulation and interference threats.

---

170 ECtHR, *Parti nationaliste basque – Organisation régionale d'Iparralde v. France,* 2007, para. 47. cited after Uerpmann-Wittzack, p.176. The ECtHR did not establish a violation. However, note that this does not apply to foreign funding of NGOs which cannot be banned on this ground as expressly found by the Court in *Ecodefence and Others v. Russia*, para. 118. Such careful regulation may be particularly important in light of the growing role of European Union Political parties as set out in the Charter on the Fundamental Rights for the European Union, Art. 12(2).

171 According to the Common Rules against Corruption in the Funding of Political Parties and Electoral Campaigns adopted by the Committee of Ministers of the Council of Europe in 2003: "States should specifically limit, prohibit or otherwise regulate donations from foreign donors." (Arts. 7 and 8 Common Rules). See also below.

172 Uerpmann-Wittzack, p. 173.

173 Council of Europe, Guide on Article 14 and on Article 1 of Protocol No. 12

174 See case law of the ECtHR concerning the protection of personal data, Ibid.

175 "In view of the intensification of the threat and the responsibilities placed on local elected representatives, the Parliamentary Delegation on Intelligence recommends that in each département, at the initiative of the Prefect and in conjunction with the territorial internal security services, an awareness-raising session for local elected representatives on the risks of interference be organised the day after each local election (municipal, département and regional). (Recommendation 5), See French Senate, Rapport de la délégation parlementaire au renseignement pour l'année 2022-2023.

176 See on this matter the EU 2016 Joint Framework on countering hybrid threats, the 2018 Joint communication on increasing resilience and bolstering capabilities to address hybrid threats and their related progress reports, the 2023 European Commission Defence Democracy Package and the European Parliament Resolution of 1 June on foreign interference in all democratic processes in the European Union, including disinformation (2022/2075). See also Matthias Kachelmann and Wulf Reiners, The European Union's Governance Approach to Tackling Disinformation – protection of democracy, foreign influence and the quest for digital sovereignty, L'Europe en formation, Summer 2023.

## 1. Measures applicable to illicit foreign funding

85. Foreign financial interference relates in particular to the regulatory framework applicable to the funding of political parties, candidates and election campaigns. As regards rules and best practices, a difference can be made between the overall regulatory framework as regards political party and campaign finance and specific rules against foreign funding. To ensure equal opportunities and protect voter freedom, overall measures such as limits on private donations and campaign expenditures, and reasonable spending restrictions, [177] promote a competitive, pluralistic democracy and a level playing field for parties. In addition, specific instruments directed specifically against illicit foreign financing activities can work as safeguards against disproportionate influence through foreign financial interference.

86. As mentioned above, illicit foreign funding can take many shapes. Efforts to prevent and address such interferences centre, on the one hand, around broad anti-corruption and transparency standards, with a specific focus on regulating political party finance, including campaign funding. While there are no specific international instruments governing foreign financial interference, insights can thus nonetheless be drawn from existing frameworks and soft law standards in the field of political party and campaign finance.

87. The United Nations Convention against Corruption encourages transparency in the funding of political parties and candidates, but does not address local and regional levels.[178] While UNCAC is applicable to all candidates in elections, [179] the Council of Europe Criminal Law Convention, more restrictively, sets standards for candidates who are office holders already by requiring measures to be taken at national level against active and passive bribery of domestic public officials and members of domestic public assemblies[180] which can facilitate such interference. The Criminal Law Convention does not address neither the local nor the national levels. The GRECO's 2022 General Activity Report connected lacking transparency with corruption, bribery and foreign interference, and emphasised the need to bridge existing gaps in legislative and institutional frameworks to effectively address foreign interference risks, e.g. through unregulated lobbying.[181] Specifically on the local and regional level, the issue of transparency and corruption was addressed by the Congress of Local and Regional level more generally in a report 'Preventing corruption and promoting public ethics at local and regional levels'.[182]

88. These standards on illicit foreign funding are further elaborated and detailed by various (soft law) documents, mostly adopted in the framework of the Council of Europe. Indeed, the Council of Europe has long recommended the prohibition of funding of political entities by foreign actors, as stated in Article 7 of the Committee of Ministers Recommendation (2003)4, on common rules against corruption in the funding of political parties and electoral campaigns, which determines that, "States should specifically limit, prohibit or otherwise regulate donations from foreign donors",[183] a recommendation

177 Para. 19 of the 1996 UN Human Rights Committee General Comment No. 25 to Article 25 of the International Covenant on Civil and Political Rights (ICCPR).
178 Ratified by 41 Council of Europe member states, UNTC, United Nations Convention against Corruption
179 In this light, the UN Technical Guide to UNCAC notes that a number of States Parties have set up one or more public bodies to be responsible for registering voters and managing elections, registering parties, monitoring party finances, reviewing candidate eligibility and financial disclosures, administering campaign finance laws and investigating any associated offences. Further, the Guide names concrete issues to be addressed to encourage transparent funding, including identification of donors (including whether or not anonymous, overseas and third-party donations or loans are permissible, restricted or prohibited), UN Technical Guide to UNCAC, 2009, II.6. pp. 17-18.
180 Including mayors or directly and indirectly elected or appointed representatives of administrative and legislative bodies on local, regional or national level. Paras 28 and 44 of Explanatory Memorandum to the Convention. Correspondingly, Arts. 2, 3 and 4 of the Convention stipulate that states enact legislative and other measures to criminalise the promising, offering or giving, as well as the request, receipt or acceptance of any undue advantage by a public official or member of a domestic public assembly in order to act or refrain from acting in the exercise of their public duties. According to the Explanatory Report to the Convention, the undue advantage need not necessarily be given to the public official himself: it can be given also to a third party, such as a relative, an organisation to which the official belongs, the political party of which he is a member. "Receiving" may for example mean the actual taking of the benefit, whether by the public official himself or by someone else for himself or for someone else.
181 GRECO, 23rd General Activity Report, pp. 19-20,.
182 Council of Europe Congress, Preventing corruption and promoting public ethics at local and regional levels, 2016.
183 CoM REC(2003)4. State regulations on donations to political parties should encompass provisions to avoid conflicts of interest, ensure transparency, prevent bias against political entities, and safeguard their independence. (Art. 3.a. See also the Council of Europe's Parliamentary Assembly made a Recommendation on Financing of Political Parties).

also regularly voiced by the Venice Commission.[184] Additional provisions on preventing and countering foreign interference in elections by financial means are contained in the PACE report on transparency and regulation of donations to political parties and electoral campaigns from foreign donors.[185] Overall, these texts agree that undue financial influence should be prohibited, a fortiori from foreign sources, especially in the light of recent reports about improper or illicit interference through financial contributions by foreign States or State-linked entities to political parties and electoral campaigns.[186]

89. As a result, most member States of the Council of Europe have explicitly banned foreign financing of political parties, to the notable exceptions of Belgium, Denmark, Sweden and Luxembourg and Austria, which do not have an outright ban on foreign donations, while Germany allows them up to EUR 1 000.[187] Such systems often lead to party/campaign finance being relatively unregulated nor audited/sanctioned. The same group of states and three other democracies do not ban foreign donations to individual candidates (Spain, Norway, Cyprus). Some countries, such as Denmark, Spain, Romania, Norway, Türkiye, only have provisions for banning anonymous donations to parties (sometimes over a relatively high threshold) but not to candidates,[188] leaving an important part of the electoral process unregulated. [189] Very recently, as US President Trump's threats to "buy" Greenland became more acute, the autonomous region of Denmark feared interference in its early elections and moved to ban foreign funding.[190]

90. Even in the event of bans being in placed, several challenges persist including on regulating political activities of elected representatives outside of campaign periods[191] or defining what constitutes in the law a contribution from foreign sources (in-kind and not only financial contributions for instance), as malign interference easily finds gaps in legislation.[192] Relatedly, as regards the local level,[193] the Congress of Local and Regional Authorities' report "Preventing corruption and promoting public ethics at local and regional levels" emphasises the need for tighter controls also over campaigning activities financed and organised outside the scope of election funds, such as by using administrative resources and unequal access to the media, and through publishing information on the financing sources of election funds.[194]

91. Still, in order to establish whether the prohibition of financing from abroad is problematic in the light of Art. 11 ECHR, every individual case has to be considered separately in the context of the general legislation on financing of parties as well as of the international obligations of a State.[195] One argument

184 See Venice Commission, Guidelines on Political Party Regulation, Second Edition, 2020 and CDL-AD(2006)014 Opinion on the Prohibition of Financial Contributions to Political Parties from Foreign Sources, 2006. In this opinion, the Venice Commission states that the prohibition of foreign funding to political parties could be considered necessary in a democratic society when foreign funding undermines the fairness or integrity of political competition, leads to distortions of the electoral process, poses a threat to national territorial integrity or when it inhibits responsive democratic development.
185 Council of Europe PACE, Transparency and regulation of donations to political parties and electoral campaigns from foreign donors, 2021.
186 PACE, Resolution on Transparency and regulation of donations to political parties and electoral campaigns from foreign donors, 2021, para. 5. See also the joint *OSCE/ODIHR and Venice Commission Guidelines on Political Party Regulation*. Likewise, the Guiding principles of the Venice Commission Guideline note that: "It is perfectly understandable that a state should be reluctant to allow a foreign country to interfere with its domestic politics by making funds available on a discretionary basis to certain of its political parties." (p. 10)
187 International IDEA, Database on Political Finance, updated as 2022.
188 GRECO, Third Evaluation Round, Country Report on Denmark, Second Addendum Report (2022).
189 "Although 70 percent of countries impose some ban on foreign donations, 37 per cent have no prohibition on anonymous donations to candidates, making it impossible to detect or stave off foreign-sponsored political finance intended to influence elections". "How OGP members can counter covert foreign political finance", VALLADARES J., SAMPLE K. for NDI, Transparency Intenrational and Open Government Partnership. August 2022.
190 Bryant M. "Greenland plans to ban foreign political funding over Trump-led election fears", The Guardian, 3 February 2025.
191 Recommendation of the Council of Europe's Committee of Ministers on Common Rules Against Corruption in the Funding of Political Parties and Electoral Campaigns, Art. 8.
192 See PACE Resolution on Transparency and regulation of donations to political parties and electoral campaigns from foreign donors, 11.4) including financial contributions to foundations, associations, charities, religious organisations and other non-profit or non-governmental organisations within the regulatory framework governing financial contributions to political parties and campaigns, whenever these organisations take part in campaigns or finance political parties.
193 Highlighting the lack of transparency in the financing of the election funds of parties and candidates can create an opaque electoral process. This opaqueness can be exacerbated by the use of funds linked to political parties which accumulate a significant proportion of party funds, but whose donors are not publicly disclosed.
194 Congress of Local and Regional Authorities, Preventing corruption and promoting public ethics at local and regional levels, 2016, para. 51. Moreover, the equal competition between the government and the opposition can be damaged by penetration of illegal funds into politics, stemming for example from foreign sources and organized crime (para. 47).
195 Para. 34. Widely accepted international or regional legal texts and standards, such as Art. 11 of the ECHR must be respected, as well as the obligations emanating from membership of the EU." Para. 13 of the Venice Commission Guidelines/Opinion.

for a less restrictive approach is e.g. foreign funding in relation to the co-operation of political parties within the European Union and its institutions. Co-operation of this kind is "necessary in a democratic society".[196] A further, general exception should also be made for donations/contributions from nationals living abroad.[197] An absolute no-go, conversely, is, as stated in the Venice Commission's Code of Good Practice in the field of Political Parties, that (even legal) private donations have as a consequence to influence or alter a party's programme.[198] A fortiori, again, this applies to foreign funding. An interesting example is the possibility for Northern Ireland parties to receive funds from both UK and Irish actors.[199]

92. A good example as regards a comprehensive (and evidently necessary) attempt to counter foreign financial interference may be the Republic of Moldova's ban of the foreign funding of candidates and political parties in elections, including municipal elections, following widespread reports of Russian meddling. Adopted ahead of the local elections in the Republic of Moldova, the law prohibits not only foreign funding from foreigners, foreign states and international organisations, but also the provision of free services or the material support in any form, direct and/or indirect. Thus, even natural persons who are citizens of the Republic of Moldova are banned to fund parties and candidates from the income obtained from abroad. Additionally, political funding is prohibited for foreign citizens, stateless persons, anonymous persons or donors on behalf of third parties. The same provision applies to legal entities with foreign or mixed capital and legal entities from abroad.[200] The law was implemented in practice during the 2023 local elections in the Republic of Moldova which were marked by widespread accusations of foreign money originating from abroad involved in the campaign.[201] As a result, the Shor Party was found by the Constitutional Court of the Republic of Moldova to be unconstitutional as "the party and its leaders, consciously, persistently, methodically and non-transparently had been using financial means of illegal origin in their activity to distort democratic processes and undermine the existing constitutional order". The party was technically prohibited from obtaining elected mandates for five years in presidential, parliamentary and local elections on grounds that it was detrimental to the sovereignty and independence of the Republic of Moldova.

93. Ensuring transparency in political party and campaign financing is critical to safeguarding democratic integrity and curbing foreign financial interference. Measures to enhance transparency may include banning clandestine or fraudulent financial aid, [202] excluding certain opaque/non-transparent ways of transaction (such as anonymous or cryptocurrency contributions), and tightening controls on intermediary and de minimis contributions.[203] Public disclosure of donations and party accounts is essential to prevent undue influence. The Recommendation of the Council of Europe's Committee of Ministers on Common Rules Against Corruption in the Funding of Political Parties and Electoral Campaigns emphasises that states should mandate transparency, limit contribution values, and enforce donation rules to avoid circumvention. Strict accounting practices are also necessary, requiring parties to document transactions, submit accounts for independent audits, and make financial statements publicly accessible. According to the Venice Commission, parties must disclose the origins of donations and include internal mechanisms for auditing finances at all levels. [204] Collectively, these transparency

196 The Venice Commission Opinion concludes accordingly that there cannot be only one answer to the question to what extent the prohibition of a foreign political party financing may be considered "necessary in a democratic society". In light of domestic legal regulations in Council of Europe states, each case of prohibition of financing from foreign sources has to be considered separately. Due consideration must be given to the political system of the country concerned, its relations within neighbours, its Constitution and constitutional values as well as the general system of financing of political parties.
197 C.f. Venice Commission Guidelines on the financing of political parties and the Venice Commission Opinion on the prohibition of financial contributions to political parties from foreign sources which both stipulate that donations to political parties and contributions to electoral campaigns from foreign states or enterprises should, in principle, be banned but this prohibition should not prevent financial donations and contributions from nationals living abroad. Guidelines 6 and 10. According to the report and guiding principles to the Guidelines, many states have, as a matter of principle, introduced a strict, mandatory ban on the funding of political parties by foreign entities or the acceptance of financial or material aid from foreign sources, whether another state, a foreign political party or foreign individuals or corporate bodies (e.g. Armenia and Russia).
198 Venice Commission, Code of Good Practice in the field of Political Parties, para. 40.
199 Political party donations and loans in Northern Ireland, The Electoral Commission, United-Kingdom.
200 Art. 26, para. 6, letter b), c), f), g) of the Law on Political Parties nr. 294, of 21. 12. 2007.
201 Besides outright cases of foreign money being distributed directly to voters and candidates during the campaign – e.g. the Congress noted during the election observation mission to the local elections in the Republic of Moldova in 2023 cases of candidate buying when pro-Russian parties paid 100€+ for candidates to be present on their lists; see above, Part III - more nuanced instances of political parties with illegal foreign funding were disclosed Venice Commission and ODIHR Opinion, 2023.
202 The *Venice Commission's Code of Good Practice in the field of Political Parties* states that "No party may receive clandestine or fraudulently obtained financial aid." Ibid., para. 42.
203 Further ways are proposed in PACE Resolution on Transparency and regulation of donations to political parties and electoral campaigns from foreign donors.
204 Venice Commission Code of Good Practice in the field of Political Parties, para. 40.

and accountability measures can contribute to deter illicit foreign funding and protect the integrity of electoral processes.

94. As regards financing regulations and especially concerning transparency in the financing of political campaigns, Lithuania constitutes a good example: While most Council of Europe states have general spending limits established on national level, Lithuania has specifically regulated the financing of political campaigns in a decentralised manner, at the level of municipalities.[205] While Lithuanian laws allow the financing of campaigns from private domestic sources, parties and candidates may not receive contributions from legal entities or foreign sources.[206] In addition, all campaign finance transactions must be made via a dedicated bank account. Cash donations as well as donations by third parties are prohibited.[207] In general terms, the aim of these regulations is to generally enhance transparency of election finances, ensure equal opportunities and reduce room for undue interferences with the political process. The latter objective is of particular relevance in the Lithuanian context as the country's political system is exposed to malign influence from neighbouring Russia which instrumentalises the Russian speaking minority in Lithuania.[208] The relevant regulations in Lithuania apply to participants in the electoral process, including politicians and political parties in each of the 60 municipalities, and are based on the number of voters in each municipality.[209]

95. Finally, independent oversight and sanctioning institutions are also necessary to curb foreign funding. Such institutions must be equipped with comprehensive competences and according equipment.[210] Independent monitoring, along with specialised personnel in combating illegal funding practices, is imperative.[211] The Congress witnessed the importance of such well-trained institutions and cooperation with law enforcement bodies in the context of the 2023 local elections in the Republic of Moldova. Moreover, effective, proportionate and dissuasive sanctions are considered key in case of violations.[212] Sanctions can go from fines to ineligibility and the annulment of an election. Furthermore, at local and regional levels, restrictions and sanctions that apply for national campaigns are often eased to facilitate participation of a wider range of actors. Oversight of party and campaign finance at these levels remain particularly challenging for two key reasons: the number of candidates/parties involved in the elections and the cost to bear for small parties to pay for external auditing of the accounts. Some countries have therefore put in place different reporting requirements for smaller municipalities (France for instance does not require reporting for municipalities under 9 000 inhabitants, which represents 33 769 municipalities).

### 2. Combatting information manipulation: the need for coordinated approaches and awareness raising

96. In the context of information manipulation, three key points can be addressed to ensure freedom of expression (Art. 10 ECHR) and to protect elections from interferences by foreign actors: the fight against disinformation per se, the impartiality of the media in the context of political advertisement and the awareness among the population to critically assess the content they are being exposed to.

205 Lithuanian Law on Funding of, and Control over Funding of, Political Campaigns, Art. 14 – Political campaign expenditure and spending limits.
206 Ibid., Arts. 7-13.
207 Ibid.
208 The national Threat Assessment by the Defence Intelligence and Security Service under the Ministry of National Defence of the Republic of Lithuania (AOTD) and the State Security Department of the Republic of Lithuania (VSD), 2024,
209 See particularly the Law on Funding of, and Control over Funding of, Political Campaigns, as well as pertinent regulations contained in the Law on Elections to Municipal Councils.
210 PACE Resolution on Transparency and regulation of donations to political parties and electoral campaigns from foreign donors: 11.10) strengthening the independence of authorities responsible for auditing political parties and campaigns, as well as improving their equipment.
211 Recommendation of the Council of Europe's Committee of Ministers on Common Rules Against Corruption in the Funding of Political Parties and Electoral Campaigns, 2003, Arts. 14-15.
212 Recommendation of the Council of Europe's Committee of Ministers on Common Rules Against Corruption in the Funding of Political Parties and Electoral Campaigns, 2003, Art. 16: Effective, proportionate, and dissuasive sanctions should be imposed for violations. Art. 16.

### 2.a. Fighting disinformation

97. As detailed above, states have a reasonable leeway for restricting electoral disinformation (especially when it comes from foreign sources) without being found in violation of Art. 10 ECHR. [213] The ECtHR's interpretive approaches consistently emphasise the need for a vigorous yet fair political debate. Accordingly, provided these restrictions are proportionate and do not result in blanket denials of access to media, it is unlikely that restrictions intended to protect pre-election periods from distortion by false narratives and computational propaganda would be questioned from an ECHR standpoint.[214] A key consideration respectively is, that states must not impose restrictions on disinformation in an indiscriminate manner.[215] To reduce the danger of information manipulation through foreign interference, a plurality of political voices should be given a platform.[216]

98. As mentioned before, little research has been done on information manipulation in the context of local and regional elections, despite the potential impact of such acts. A good practice was tested in Norway, with post-election research being commissioned by the Ministry of Local Government, on disinformation campaigns on social media in the context of the 2023 Norwegian municipal council and county elections.[217] While the research did not show systematic foreign disinformation, it provided interesting insights on opportunistic behaviours online. Similar research had been commissioned in 2019 and also pointed to limited interest of foreign actors in local elections in Norway, but mentioned the challenge of covert networks for democracy, including at local level.[218]

99. An additional factor to be acknowledged is, obviously, the debate outside "traditional" media channels. In light of the increasing role of social media/private actors, including in the context of new (and emerging) technologies, private/third party actors (social media platforms, digital/online platforms) turn increasingly relevant stakeholders to be taken on-board. The unique nature of the online environment demands that states and local authorities consider co-regulation. In pursuance of its obligation to protect, a state may (and at times even must) oblige private actors as internet news portals,[219] e.g. ordering an internet portal operator to remove comments posted by a third party.[220]

100. After interference in the 2017 French presidential election, France adopted a stricter approach to counter foreign electoral interferences. In 2018, the "Law Against the Manipulation of Information" was passed with the goal of addressing the threat of disinformation that could mislead the public.[221] Defined as the "inexact or misleading allegation of a fact intended to alter the sincerity of an upcoming vote and spread deliberately or massively online," the law operates on several (relevant) principles.[222] The first principle focuses on the responsibility of digital platforms. These platforms, particularly those with a large user base, are required to actively combat disinformation. The law encourages them to enhance the transparency of their algorithms, promote content from verified sources such as press agencies, and work to shut down accounts that spread false information.[223] Another principle of the law introduces

213 Note, respectively, that the ECtHR case law (as discussed in Part V) is not the only interpretive framework for protecting freedom of expression in laws designed to combat electoral disinformation. Also, the EU and its Charter of Fundamental Rights provides for relevant standards. Still, a comprehensive analysis would have exceeded the scope of this report. Importantly, many Contracting Parties to the ECHR are also EU Member States and are, therefore, subject to EU law. National laws in Europe that aim to restrict disinformation in the online context must navigate the evolving contours of EU laws (notably DSA) on intermediary liability. The standards in the EU Fundamental Rights Charter roughly conform to those in the ECHR.
214 See also Venice Commission, The impact of the information disorder (disinformation) on elections,
215 Shattock, Free and Informed Elections? Disinformation and Democratic Elections Under Article 3 of Protocol 1 of the ECHR, 2022,.
216 Ibid., 6.6.5.
217 Common Consultancy, Report: Mapping foreign influence on social media before, during, and after the Norwegian municipal council and county elections 2023, 15 January 2024 (available in Norwegian only).
218 Kroglund, Preben Svarva, Constructing Online Disinformation and Misinformation in Norway The discourse of causes, imaginaries of futures and interpretations of solutions, Norges teknisk-naturvitenskapelige universitet, May 2021.
219 Which was also addressed by the ECtHR in the context of Art. 10. While, because of the particular nature of the Internet, the "duties and responsibilities" that are to be conferred on an Internet news portal for the purposes of Art. 10 may differ to some degree from those of a traditional publisher as regards third-party content (ECtHR, *Delfi AS v. Estonia [GC],* para. 113.
220 More specifically, the ECtHR has identified four criteria with a view to striking a fair balance between the right to freedom of expression and the right to reputation of the person or entity referred to in the comments in ECtHR, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, paras. 60 et seq.; ECtHR, *Delfi AS v. Estonia* [GC], paras. 142 et seq., namely: 1. the context and contents of the comments, 2. the liability of the authors of the comments, 3. the measures taken by the applicants and the conduct of the aggrieved party, 4. the consequences for the aggrieved party and for the applicants. Shattock 2022, pp. 6-7. See Part V.
221 LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.
222 Ibid., Art. L. 163-2.-I.
223 Ibid., Arts. 1-4.

a legal mechanism to address disinformation during elections. If false or misleading information is circulating that could affect the fairness of the vote, legal action can be taken to bring the case before a judge.[224] The fourth principle strengthens the role of the French broadcasting regulator. If the regulator detects a foreign-controlled or influenced media outlet spreading disinformation during the electoral period, it has the authority to request the suspension of the media service until the voting process is completed.[225] Altogether, the law aims to safeguard democratic processes by creating transparency, accountability, and tools to combat the growing threat of disinformation.[226]

101. To safeguard the integrity of online services, platforms should implement measures to combat bots, fake accounts, and the spread of political disinformation.[227] However, these actions must be balanced with the protection of human rights, including freedom of expression, anonymity, and the confidentiality of private communications.[228] Transparency should also extend to the labelling of automated accounts, making it clear when interactions are not human-driven.[229] Clear and predictable policies should guide the maintenance of service integrity, especially in countering disinformation. Any restrictions on content access, particularly during elections, should be transparent, non-discriminatory, and limited to the minimum necessary to avoid unjustified limitations on legal content.[230] To further reduce the spread of political disinformation, states should push for stricter oversight of advertisement placements, curbing the financial incentives for those who spread false information.[231] During election periods, states may also impose rules like electoral silence or bans on conduct and publication of opinion polls.[232]

102. Many good practices on the fight against disinformation coexist in Europe but overall, states are encouraged to work closely with online platforms and civil society organisations to counter deceptive speech. Relevant authorities should regularly engage in transparent and inclusive consultations with all stakeholders. This dialogue is essential for balancing the public interest, user needs, and industry concerns. In Spain, a public-private collaboration working group was established to tackle information security during elections and it includes public and private interlocutors as well as civil society members.[233]

103. In addition, a coordinated approach can be very useful to debunk coordinate mis or disinformation campaigns. In Bosnia and Herzegovina, ahead of the 2022 general elections (which include the cantonal elections), the CEC responded to online attacks and fake news by establishing a crisis communication strategy, tailored to social media and it also conducted a pre-election threat assessment.[234]

### 2.b. Promoting transparent and equal coverage of political contestants and network neutrality

104. Recommendation CM/Rec(2022)12of the Committee of Ministers to member States on electoral communication and media coverage of electoral campaigns establishes good practice related to equal coverage of contestants. Overall, it provides that the access to media and political advertising should be provided fairly and transparently to all electoral contestants, ensuring no undue promotion for political actors (a fortiori for contestants favoured by foreign powers). It states that oversight mechanisms should be established to monitor online platforms, supported by independent advisory bodies and equipped with resources to monitor content moderation. Authorities should be empowered to issue timely, proportionate, and graduated sanctions as necessary to address violations. This is particularly

224 The judge has 48 hours to determine whether the content should be removed, provided it meets the criteria of deliberate, massive manipulation designed to influence the vote. Ibid., Arts. 11-15.
225 Ibid., Arts. 16-19.
226 See for instance Guillaume, Hybrid CoE Strategic Analysis 16 Combating the manipulation of information – a French case, 2019.
227 Recommendation CM/Rec(2022)12, 4.4.2.
228 As guaranteed by Art. 10 of the Convention.
229 Recommendation CM/Rec(2022)12, 4.4.3.
230 In line with Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries.
231 Recommendation CM/Rec(2022)12, 4.4.5.
232 Ibid, 4.4.6.
233 Andrej Poleščuk, Veronika Krátka Špalková, Hybrid CoE Research Report 10 Preventing election interference: Selected best practices and recommendations, 2023.
234 Daria Azariev North, David Levine, Krystyna Sikora and Nikoleta Diossy, Building Resilience Against Election Influence Operations: Preparing for the European elections in 2024 and beyond, GMF/Alliance for Securing Democracy and IFES, April 2024.

important when it comes to actions like blocking accounts or removing content that could unduly influence election campaigns or violate electoral rules.

105. Transparency in online political advertising is also essential, requiring platforms and political actors to maintain detailed archives of ads, including demographic targeting information, and tools should be developed to monitor compliance and detect inauthentic behaviour. States should also ensure fair access to online political advertising and update election regulations to address the growing role of digital platforms in campaigns.

106. Transparency and accountability relating to the use of algorithms, content curation, content moderation and handling of problematic accounts are also key to protect voters from undue influence. The algorithms used by both public and private entities to rank, display, and moderate political ads and electoral content must be transparent and verifiable. To align with international human rights standards,[235] states should adopt co-regulatory frameworks that promote accountability and fairness in algorithmic decision-making.[236] Moreover, creating opportunities for multistakeholder engagement is essential. Civil society, political parties, and other stakeholders should have a voice in addressing concerns about the deployment of algorithms, particularly in the political and electoral context.[237] Online platforms, under these frameworks, must also be required to publish transparency reports and reports on their moderation systems.

107. States must carefully assess the impact of microtargeted political advertising on citizens' voting behaviour. This includes considering how such advertising affects access to diverse information, exposure to a range of political perspectives, and the fundamental right to freely express political opinions and make informed choices.[238] To address these concerns, it is essential for states to ensure that their data protection laws and policies are rigorously applied in the context of electoral campaigns, aligning with established privacy and data protection standards.[239] Online platforms should also disclose clear and detailed information to users about the reasons for their targeted political advertisements. [240]

### 2.c. Strengthening voter and citizen education

108. As a long-term measure to combat the impact of information manipulation, voter and citizen education is a good tool available to all levels of government and an opportunity to share correct electoral information and good habits to detect disinformation from both foreign and domestic sources. Relevant awareness-raising, information and education campaigns should be conducted accordingly.[241] Indeed, media and information literacy, encompassing digital skills and critical thinking, is crucial for effective citizenship in today's online world and for informed political participation, whether as voters or candidates. These skills enable citizens to seek out, acquire, and assess information from a variety of sources. In this area, both public and civil society initiative to work on electoral integrity and voter awareness should be encourages, as civil society can highly contribute to detect and counter disinformation campaigns. Citizen observers are well-equipped to investigate and map disinformation trends, as they understand the legal framework and the vernacular, but they can also increase awareness among the population by releasing reports and guidelines.

109. To foster these competencies, local and regional authorities tasked with school curricula could integrate media and information literacy into school curricula, support lifelong learning initiatives, and provide assistance to media organisations, especially public service and community media outlets.[242] Furthermore, local and regional media can serve as a transmission belt to educate voter and fact-check information. As mentioned in 2023 Congress report on Local and regional media: watchdogs of democracy, guardians of community cohesion, "Strong local and regional media can also play a role in

235 Council of Europe AI Convention, and Particularly those outlined in Recommendation CM/Rec(2020)1.
236 Recommendation CM/Rec(2020)1.
237 Ibid.
238 Ibid, 5.5.1.
239 Particularly those outlined in Convention 108 and Convention 108+.
240 Recommendation CM/Rec(2022)12, 5.5.2.
241 Recommendation CM/Rec(2022)12 of the Committee of Ministers to member States on electoral communication and media coverage of election campaigns, Principle, 6.6.6.
242 Ibid, 6.6.6.

diminishing the risk of fake news and disinformation about local government or elected officials or investigate rumours and provide local officials with a platform to provide further information."[243]

110. An example of the strengthening voter awareness can be drawn from Sweden which is actively strengthening its civil resistance to foreign interference, requiring long-term measures beyond election years. The Swedish model assumes that electoral interference is part of a broader strategy by foreign powers, and this is factored into how the country protects its electoral processes. Therefore, Sweden goes beyond merely safeguarding elections during the electoral period, implementing continuous measures immediately afterward. These efforts include public awareness raising campaigns on topics that may be exploited in disinformation campaigns and promoting media literacy. Although such activities are heightened during election years, they remain a focus throughout the electoral cycle.[244] In early 2022, Sweden established the Psychological Defence Agency (PDA), whose primary mission is to protect Sweden's open democratic society, the free formation of opinions, fundamental freedoms, and ultimately, national sovereignty. The PDA works to detect, analyse, prevent, and counter foreign malign information campaigns and other disinformation targeting Sweden or its interests. This includes attempts by foreign actors to weaken national resilience or influence public opinion and decision-making processes.[245] An example of the PDA's long-term initiatives is the national campaign "Don't Be Fooled", designed to raise awareness about misleading information and aiming to equip citizens with tools to identify and understand it. This campaign combines information dissemination with educational activities, enabling Swedish citizens to learn the basics of spotting disinformation and understanding how such campaigns operate.[246]

### 3. Electoral cyberattacks

111. While foreign electoral cyber-attacks have remained relatively limited, some good practice can be established based on soft law instruments and case studies. As detailed above, electoral cyber-attacks can occur at various (technical and administrative) stages of the electoral process, from voter registration and the election campaign to the counting of votes. It is however important to take into account that most electoral processes at local and regional levels in Europe continue to be paper-based, protecting them from potential cyber-attacks against core elements of the system and making it harder to interfere.

112. The Budapest Convention on Cybersecurity[247] covers some of the fundamental issues pertaining to elections. Indeed, electoral cyberattacks may involve the following types of conduct that may be criminalised by the Budapest Convention, such as illegal access to computer systems (Art. 2); illegal interception of non-public transmissions of computer data (Art. 3); data interference (Art. 4); system interference (Art. 5); misuse of devices (Art. 6); as well as computer-related forgery.[248] Crimes committed by legal persons that contribute to election interference are also covered under the Convention, ensuring that organisations, not just individuals, are held accountable (Art. 12). For the parties to the Budapest Convention, a firm framework regulates activities from a criminal law perspective.

113. Further layers of protection are added by privacy rights. In addition to the right to private (and family) life in Art. 8 ECHR, further standards may be found in treaties adopted in the framework of the

243 See Recommendation 498 (2023) of the Congress of Local and Regional Authorities on Local and regional media: watchdogs of democracy, guardians of community cohesion and Explanatory Memorandum.
244 Guillaume, Hybrid CoE Strategic Analysis 16 Combating the manipulation of information, 2019, p. 20.
245 The Swedish Psychological Defence Agency, 'Our mission'
246 Swedish Civil Contingencies Agency (MSB), 'If crisis or war comes', 2022.
247 Ratified by 76 states. Council of Europe, The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols.
248 One such cyberthreat is the illegal access to computer systems, where sensitive or confidential information related to candidates, campaigns, political parties, or voters is obtained without authorization in order to not only compromises privacy but potentially also influence the outcome of an election. Another form of cyberattack involves the illegal interception of non-public transmissions of computer data. This can happen when data sent to, from, or within a computer system is intercepted to access sensitive or confidential information, potentially exposing critical details about candidates or political strategies. Data interference, where computer data is damaged, deleted, altered, or suppressed, may be another element of offence at stake since it can manifest in various ways, such as modifying websites, altering voter databases, or tampering with voting machines, all of which possibly of relevance for foreign electoral interference e.g. relating to the distortion of results of an election. System interference is a tactic where the normal functioning of computer systems used in electronic voting or campaigns is disrupted. This might involve hindering campaign messaging, obstructing voter registration, or even preventing votes from being cast or counted through methods like denial of service attacks or the introduction of malware. Budapest Convention.

Council of Europe, such as the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)[249] or the Additional Protocol to the Convention of 2011 which sets standards for the establishment of data protection supervisory authorities.[250] The 2018 Modernised Convention[251] reinforces data protection principles by stipulating that data must be processed fairly and transparently, collected for explicit, specified, and legitimate purposes, and not processed in a manner incompatible with these purposes.

114. In addition, there are several recommendations especially as regards the prevention of cyber-attacks which may be derived from soft-law standards. The Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States (2022) provide strong guidelines to secure ICT systems used in electoral processes. First, states have a duty to ensure that the ICT solutions used in the electoral process are both available and reliable. This means that these systems must function as intended, even in the face of cyberattacks. If any problems do nonetheless occur, fall-back solutions need to be quickly activated, including those that do not rely on active connections.[252] An example of good practice can be drawn from local elections in Catalonia, where mobile teams of IT engineers were trained and deployed and had to report any glitch in the vote tabulation system.[253]

115. States must ensure that ICT technologies used in elections provide secured, accurate and authentic information, with robust authentication mechanisms to prevent unauthorised interventions. Independent integrity checks and responsive protocols are essential to detect, correct, and respond to cybersecurity threats, safeguarding elections from external attacks and internal breaches. The ability to detect and correct errors or manipulations is crucial throughout all phases of the electoral process, from managing voter rolls to tallying votes and transmitting results, particularly when transmission occurs over the internet.[254] An example of good practice can be found in training IT engineers, operators and/or election administration staff to detect these attacks and to set up contingency plans. Ahead of the 2024 local elections in Bosnia and Herzegovina, a workshop was held on ICT systems used in the elections and contingency plans were discussed.[255]

116. As other stakeholders such as political parties are involved in the process and can be the target of attacks, it is also important to promote good cyber-practice for political parties, in particular in the face of malware, DDoS and spear phishing. A good practice in this regard is the guidelines developed by the National Cyber Security Committee of Ireland ahead of the local and European elections held in June 2024. These guidelines recall the key risks, propose some prevention measures and clarify steps to follow in case of cyber-attack.[256] In Finland, local administrative bodies also receive cyber security training, while citizens can be provided with online training regardless of the election cycle.[257]

117. In addition to making systems accountable, compliant with human rights and data protection standards, transparent in case of malfunction and free of interferences, continuous risk monitoring and management is essential to protect the systems from being breaches/modified by foreign actors.[258] Critical electoral processes, especially those relying on web-based solutions, face risks that need to be

249 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).
250 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (ETS No. 181). The particular added value of this legal framework in comparison with the European Union General Data Protection Regulation is that, being open to any country in the world, it allows various legal systems to stand under the same umbrella.
251 Amending Protocol (CETS: 223) to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).
252 Council of Europe Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States, 2022, Guideline 5.
253 The team had direct communication with the systems, development, communications, security, forensic, and DOS teams. Regular meetings were established every three hours to review the security status and concentrate on a brief report. When the counting of votes began, the meetings were held every hour. If any suspicious equipment was detected, it was included in a quarantine network for forensic review. For all teams, a limited number of fully operational back-ups were available to replace any suspect equipment. Source.
254 Ibid., Guideline 4.
255 https://www.venice.coe.int/webforms/events/?id=3711
256 National Cyber Security Committee of Ireland, Quick Guide: Cyber Security Best Practice for Electoral Candidates, 2024. It also prepared a more detailed guide on Cybersecurity for Political Organisations and Election Candidates ahead of the 2024 election period.
257 Andrej Poleščuk, Veronika Krátka Špalková, Hybrid CoE Research Report 10 Preventing election interference: Selected best practices and recommendations, 2023.
258 Such as those outlined in Art. 6, para. 1, of the 108 Convention.

managed effectively, with proportionate responses developed whenever security risks are identified. Evaluating current risks and determining whether the remaining risks are acceptable is an ongoing process, especially as new types of cyberattacks continue to emerge. Understanding and managing the remaining risks is crucial. Decisions must be made on how to handle these risks, and risk management strategies should include robust contingency plans.[259]

118. A good example of protection against cyber-attacks is Ukrainian voter registration. Generally, to protect voter (and candidate) registers from cyberattacks by malign foreign actors, voter registers must be constantly updated and securely protected. This also helps to safeguard their proper functionality for elections and supports the confidentiality of personal data. Ukraine stands out as a country with a strong system in place to protect its voter database from unauthorised manipulation. One of the key systems Ukraine employs is the Central Evidence of Voters, designed to safeguard the personal information of voters against unlawful edits or deletions. Not only can voters verify their own data, but they can also check limited information about others, therewith contributing to the system's transparency.[260] In addition, Ukraine takes proactive steps to ensure the integrity of its electoral processes through the Central Voters Committee (CIK). This permanent state body is part of the Central Election Commission and is responsible for organising and overseeing national as well as subnational elections in the country.[261] The protection of the Committee's infrastructure is multi-layered, designed to prevent unauthorised access or tampering. For instance, accessing the electoral register requires the simultaneous use of two keys, so that no single individual can alter data independently. Every change made to a voter's data is recorded in the registry's service fields, and the process is made transparent to the public, further discouraging unauthorised action.[262] Additional measures prevent the illicit transfer of data from the registry. Special encryption methods and tamper-proof CDs are used when transferring information to political parties and other electoral participants. These safeguards work together to maintain the security and accuracy of Ukraine's voter data, preserving the integrity of its electoral system.

119. Another good example is Lithuania, and more specifically its campaign environment. Lithuania indeed serves as a model for proactive security measures, with its National Cyber Security Centre (NCSC) routinely testing the security of both, political party websites and election infrastructure systems.[263] In addition to this, the NCSC offers online training and educational programs for politicians and candidates, therewith implementing comprehensive cybersecurity measures for political parties' digital presence. Lithuania's comprehensive approach highlights the importance of adopting a precautionary approach.

120. Notably, for e-voting mechanisms, the Council of Europe landmark Recommendation CM/Rec(2017)51 of the Committee of Ministers on standards for e-voting, established key requirements for the deployment of such solutions.[264] These include a secure and reliable process in place for aggregating all votes and calculating the final result (a critical stage of the process and most vulnerable to foreign interference through cyberattacks), that voters are able to verify that their will is correctly reflected and unaltered, and that the vote cannot be traced back to voter, ensuring the full secrecy of the vote.

121. The standards on e-voting establish that when states decide to introduce e-voting, they should do so gradually, preventing a security breach from the outset when the system may be most vulnerable to interferences leading at a later stage to more substantial cyberattacks. Transparency is also crucial in the implementation of e-voting, and states must ensure that every aspect of the process is open to external scrutiny (observers) and clear without disclosing sensitive data for protection of the system and confidentiality of voters. Furthermore, independent evaluation is advised to ensure the system fully respects the relevant legal and democratic principles, also acknowledging the cybersecurity element, i.e. technological advancements and emerging (cyber) challenges. Finally, the e-voting system must be capable of identifying any votes that are affected by irregularities, reducing the impact of potential cyberattacks which undermine the results of the elections.

259 Council of Europe Committee of Ministers' Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member States, 2022, Guideline 8.
260 Bill no. 2536-VI 'On the State Register of Voters'.
261 Decree 'On approval of the Regulations of the Central Election Commission', 26 April, 2005 No. 72.
262 Ibid.
263 Lithuanian National Cyber Security Centre.
264 Recommendation CM/Rec(2017)51 of the Committee of Ministers to member States on standards for e-voting, II. 6-9.

122. Estonia may be drawn upon as an interesting example in relation to e-voting. As regards preparedness and diligence of e-voting, it stands out in comparison to the rest of the world, offering numerous best practices. In fact, in most countries, pre-election preparations focus on voting systems or software, but few countries begin the process more than a year ahead. The high level of digital integration enabled Estonia to start holding (partially) online elections as early as in 2005.[265] This requires a comprehensive system of pre-election preparedness. Election preparations in Estonia are a collaborative process, led by the Information System Authority (RIA), the agency responsible for safeguarding the nation's digital infrastructure.[266] Trust in digital governance is fundamental, and the RIA is key to ensuring public confidence in the system. The security of Estonian elections begins with a rigorous setup phase, which includes candidate registration, updating the voter database, and preparing the election software. Most importantly, to minimise the risk of cyberattacks exploiting potential software vulnerabilities, Estonia develops new voting software for each election.[267] This proactive and thorough preparation has successfully managed to avoid breaches and violations.

## VI. CONCLUSIONS AND WAYS FORWARD

123. As this report shows, while local and regional electoral processes attract modest interest from foreign powers, these elections are not completely immune to potential foreign interference, being instances of information disinformation, opportunistic cyber-attacks and illicit funding. Foreign electoral interference is a multi-layered and complex phenomenon, which can affect the entire electoral cycle. New (and emerging) information technologies have unprecedently increased the means, ways and impact of foreign electoral interferences.

124. In light of this diversity, also the respective legal/regulatory framework is multilayered and scattered. It concerns applicable rules of international relations as the non-intervention principle as well as the European human rights framework applicable within a state. Moreover, criminal law dimensions may be at stake, as outlined in the UNCAC or the Budapest Convention on Cyber-Security. Finally, numerous soft law instruments are applicable, providing for best practices. Further best practices may be found when looking into national/domestic examples. While there are limited provisions explicitly for the local and regional context in place, the overall framework is of relevance for the local level too.

125. Three challenging elements have been uncovered for future assessment of this phenomenon. First of all, the lack of up-to-date information and research does not allow local and national authorities to fully understand and prevent such interferences. This is in part due to the difficulty to prove and attribute foreign interferences, as state actors more and more make use of hybrid tools to advance their interests, navigating between interference and influence. At the same time, the focus in literature on national-level elections can obscure the peculiarities of the local level, which in many countries represent a crucial democratic institution for citizens but can also offer other pathways for political corruption. Such assessments, while complex in nature, would allow voters, contestants and the administration alike to evaluate the situation, without overamplifying or underestimating the threats and to devise appropriate mitigation plans.

126. Second, at a time when the information environment is constantly threatened by alternative narratives, the fight against foreign interference itself is now sometimes manipulated for political purposes. Indeed, without trying to attest of the interference, some political actors have labelled their opponents as agents of foreign powers. Mutually blaming each other can only further erode the trust in democracy. The emergence of repressive foreign agents' laws throughout Europe is another strong sign that the fight against credible attempts may be further hindered. As highlighted below, careful approaches are needed to prevent abuse in terms of balancing different rights, especially in relation to the legal regulation of foreign funding (of NGOs) and the prohibition of political parties.

127. Finally, as the EU and many other countries in its wake, successfully tackled some parts of foreign interference (including illicit funding, potential cyberattacks, etc), the emergence of non-state actors,

265 Piret Ehin, Mikhel Solvak, Jan Willemson, and Priit Vinkel, 'Internet voting in Estonia 2005–2019: Evidence from eleven elections', Government Information Quarterly, Volume 39, Issue 4, October (2022),
266 Estonian Information System Authority (RIA),
267 Piret Ehin, Mikhel Solvak, Jan Willemson, and Priit Vinkel, 'Internet voting in Estonia 2005–2019: Evidence from eleven elections'.

loosely or not affiliated with one specific state, such as for instance online groups promoting extremists agenda, seems to reshuffle the deck again and to create new needs for regulation in full compliance with human rights against these groups, which are gathering significant influence.

128. Confronted with a multifaceted or “hybrid” threat, public awareness and voter education remain one of the best protections against foreign election interference at all levels of government and can in the long run participate in reducing entry of illicit funds in local politics, debunk techniques used to make voters less confidents in electoral processes and protect them and their votes from malicious attacks.