Institutions and foreign interferences

STUDY

Requested by the AFCO committee

European Parliament

Institutions and foreign interferences

Policy Department for Citizens' Rights and Constitutional Affairs
Directorate-General for Internal Policies
PE 655.290– June 2020

EN

Institutions and foreign interferences

Abstract

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the AFCO Committee, assesses the EU responses to counter foreign interferences. It examines in particular the effectiveness of the EU action against foreign interferences in the 2019 European Parliament elections, the COVID-19 crisis and the issue of foreign donations to European political parties. The study concludes with specific policy recommendations to enhance the EU's responses.

This document was requested by the European Parliament's Committee on Constitutional Affairs.

AUTHORS
Edoardo BRESSANELLI, Sant'Anna School of Advanced Studies, Pisa (Principal Investigator)
Anna DI PALMA, Sant'Anna School of Advanced Studies, Pisa
Gaetano INGLESE, Sant'Anna School of Advanced Studies, Pisa
Sofia MARINI, Sant'Anna School of Advanced Studies, Pisa
Eric REPETTO, Sant'Anna School of Advanced Studies, Pisa

ADMINISTRATOR RESPONSIBLE
Alessandro DAVOLI

EDITORIAL ASSISTANT
Ginka TSONEVA

ACKNOWLEDGEMENTS
We are grateful to Francesco Strazzari, Serena Giusti and Claire O'Neill.

LINGUISTIC VERSION
Original: EN

ABOUT THE EDITOR
Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact the Policy Department or to subscribe for updates, please write to:
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
Email: poldep-citizens@europarl.europa.eu

Manuscript completed in June 2020

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

CONTENTS

LIST OF ABBREVIATIONS

AVMSD	Audiovisual Media Services Directive
CoE	Centre of Excellence
CoP	Code of Practice on Disinformation
ECDC	European Centre for Disease prevention and Control
ECNE	European Cooperation Network on Elections
EDMO	European Digital Media Observatory
EEAS	European External Action Service
EP	European Parliament
EU	European Union
EU INTCEN	EU Intelligence and Situation Centre
EUPP	European political party
EUPF	European political foundation
FN	Front National
FPÖ	Freiheitliche Partei Österreichs
FvD	Forum voor Democratie
GDPR	General Data Protection Regulation
GRECO	Group of States Against Corruption
IDEA	Institute for Democracy and Electoral Assistance
IP	Internet Protocol
LIBE	Civil Liberties, Justice and Home Affairs
MS	Member States
NATO	North Atlantic Treaty Organisation
OSCE	Organisation for Security and Cooperation in Europe

OECD	Organisation for Economic Co-operation and Development
ÖVP	Österreichische Volkspartei
PVV	Partij voor de Vrijheid
RAS	Rapid Alert System
RT	Russia Today
TF	Task Force
VP	Vice-President

LIST OF BOXES

LIST OF TABLES

EXECUTIVE SUMMARY

Background

Foreign interferences represent a huge challenge for democratic government and society. The 2016 US Presidential elections, the 2016 referendum on EU membership in the UK, the 2017 French presidential elections are prominent illustrations of a more general and dangerous trend. While foreign interferences – which can be conceptualised as those activities carried out by, or on behalf of, a foreign actor, through a variety of means, to undermine the interests of another country – have existed for a long time, the internet and social media have provided new, fertile ground for their pursuit. Social platforms have been used effectively to wage large-scale disinformation campaigns by countries such as China or Russia, particularly ahead of new elections, with social media enabling them to cover their actions behind automated accounts or bots.

Disinformation campaigns – and narrative warfare more broadly – are widely perceived as a threat to free and fair elections both in the US and Europe. Based on the polling conducted by a Special Eurobarometer on 'Democracy and Elections', for instance, a large majority of EU-based internet users are worried or deeply worried about disinformation and misinformation, microtargeting and political advertising. At the same time, however, the same survey also shows that a majority of them are concerned about restrictions and censorship of political debates before elections. This vividly illustrates the tension between shielding elections from disinformation and the danger of hampering freedom of speech and media pluralism, as well as the difficult balance that policy makers and regulators have to strike.

Disinformation is a prominent, but not the only type of foreign interference. The funding of political parties or campaign organisations by foreign states may be another disruptive factor for democracies. Here again, there are several examples of mainly far-right populist political parties supported by foreign funding. From the Leave.EU campaign organisation in the Brexit referendum to the League in Italy, financial resources from abroad have allegedly been used, often exploiting 'grey areas' in the national legislation on party financing. A notable recent development, even in countries with more liberal traditions on party funding, is the tendency to strengthen regulations and limit or ban funding from abroad.

The EU has developed its policies and tools to tackle foreign interferences considerably. As Russian action vis-à-vis Ukraine and the Eastern region became more aggressive in 2014, the EU stepped up its efforts to counter hybrid threats, disinformation and election interferences. The protection of the 2019 European Parliament elections – which took place in an already difficult context for the EU, with the surge of Eurosceptic and anti-EU forces – became paramount, with several actions implemented to improve coordination with the Member States and cooperation with NATO.

The outbreak of the covid-19 epidemic dramatically showcased the importance of an effective and prompt response by the EU to narrative warfare and alternative information campaigns waged by countries like Russia or China, set-up with the purpose of undermining the trust of European citizens in their democratic systems and in the EU.

Aim

The study aims to provide background information, map the institutional and policy responses, and assess the performance of the actions and tools set up to tackle the challenge of foreign interferences in the EU.

Chapters 1 and 2 conceptualise foreign interferences, discuss their impact on democratic processes and, describing the EU's responses, prepare the ground for the empirical chapters. Chapter 1 of the study provides the general background to understand the nature and different types of foreign interferences and the challenge that they pose to, and for, liberal democracies. A specific focus will be placed on Russia and hybrid warfare. The strategies endorsed by international organisations and other democratic states to tackle foreign interferences are also discussed.

Chapter 2 maps the strategic positions and actions taken by the EU institutions - the European Council, the Council of the EU, the European Commission and the European Parliament - to tackle foreign interferences. It places its analytical focus mainly on hybrid threats, disinformation and strategic communication. It also provides a state-of-the-art presentation of the current agenda and reforms based on the strategic agenda of the von der Leyen's Commission and the 2019 resolution of the EP on foreign interferences.

Chapters 3 and 4 deal with two critical cases to empirically assess the capacity of the EU to respond to foreign interferences and disinformation specifically. Chapter 3 analyses the 2019 EP elections. It takes an in-depth look at the election package of the European Commission, the Code of Practice on Disinformation, the monitoring activity and communication strategy of the StratCom Task Forces and the new Cooperation Network on Elections. Based on a wide array of sources - reports by the EU institutions, think-tanks and academic studies - the chapter attempts an evaluation of the performance of these instruments in the run-up to the May EP elections.

Chapter 4 deals with the timely case of the COVID-19 epidemic. Based on the reports of the EUvsDisinfo project of the EU East StratCom Task Force and other independent sources, the chapter maps the narratives spread by foreign states and actors. The chapter reviews and provides an early assessment of the responses of the EU.

Chapter 5 moves the focus to political parties and foreign interferences. It provides background information on recent cases of parties or campaign organisations receiving financial resources from abroad. It also reviews the national regulations on party funding with respect to foreign donations. Finally, the chapter moves to the EU-level and discusses the recent reforms in the regulation on party statutes and funding.

Chapter 6 concludes with specific policy recommendations emerging from the analysis. An effective strategy to counter foreign interferences should be comprehensive, focusing both on strategic communication and institutional responses, and on social development. Private and public, economic, political and social, national, sub-national and international actors should all be involved and should contribute to its successful implementation.

1. FOREIGN INTERFERENCES AND DEMOCRACY

KEY FINDINGS

- Foreign interferences are defined on the basis of two elements, malicious intent and lack of transparency, and cover a variety of hybrid methods that foreign actors employ to penetrate domestic politics;
- Democracies are the main targets of foreign interferences, which are generally carried out by autocratic actors in asymmetric contexts. These operations exploit the structural vulnerabilities of democracies - i.e. advancing technology, social and economic openness - and threaten liberal core values, human rights, as well as the good functioning of societies and institutions, both at the national and at the EU level;
- Russia has been the main player behind the systematic use of foreign interferences. Their effects can be evaluated in multiple countries, both inside and outside the EU – the U.S., Ukraine and Estonia are among the main examples;
- The international community and a growing number of national governments are progressively gaining awareness of the challenge posed by foreign interferences. In response, new specific tools and actions have been implemented.

1.1 Introduction

Foreign interferences are a growing challenge for democracies all around the globe, exploiting their vulnerabilities and openness – i.e. the open market, freedom of expression – threatening core liberal values and damaging the political, social, and economic democratic model in its cohesion and efficiency.

This phenomenon is not new. It has always existed in the history of international relations, although it has evolved over time and adapted to new geopolitical contexts and changing warfare methods. Indeed, by looking at its constitutive elements - the malicious intent to disrupt and destabilize the target and the lack of transparency - it is reasonable to state that foreign actors have traditionally been engaged in this type of operation. However, advancements in technological knowledge and the advent of social media have pushed for a change in the type of foreign interferences. In fact, both state and non-state actors have been gradually adopting a variety of new unconventional, subtler but equally invasive tools to weaken the target. This often happens in asymmetrical contexts, where the actors have different military, economic and political resources, and the inferior power searches for new strategies to surprise the stronger enemy. This idea was explained by Sun Tzu, in his classic *The Art of War:*

> *'If your enemy is secure at all points, be prepared for him. If he is in superior strength, evade him. If your opponent is temperamental, seek to irritate him. Pretend to be weak, that he may grow arrogant. If he is taking his ease, give him no rest. If his forces are united, separate them. If sovereign and subject are in accord, put division between them. Attack him where he is unprepared, appear where you are not expected'.* [1]

[1] Tzu, S., *The Art of War*, Shambhala Publications, London, 1988, Chapter 1.

These concepts are perfectly applicable to contemporary foreign interferences, which are frequently carried out by autocratic state and non-state actors to destabilize the international order and weaken liberal democracies, which are often unprepared to tackle the challenge.

This chapter provides background information and a conceptual introduction to the topic. Section 1.2 defines 'foreign interference' and analyses its main implications for the functioning and the stability of democratic systems. Section 1.3 provides some empirical evidence, focusing mainly on the current Russian hybrid strategy, targeting Western countries and the EU. Section 1.4 summarises the state of play and concludes.

1.2. The challenge for democracy

Foreign interferences are an evolving phenomenon. A thorough understanding of the concept of foreign interference and its empirical manifestations is a crucial preliminary step to assess the policies implemented to counter them and provide concrete policy recommendations.

To begin with, a definition of "foreign interference" should differentiate hostile actions from ordinary political practices, while accounting for the variety of tactics employed. The EU employs different terms. While the European Commission President Ursula von der Leyen refers to 'external interferences',[2] the term 'manipulative interference' appears in some documents of the Council.[3] In its resolutions and studies, the EP has adopted the labels 'foreign interference'[4] and 'foreign influence operations'.[5] Looking at the concrete manifestations of the concept, the October 2019 EP resolution gave some examples of how 'foreign interference' could be observed empirically:

> *Foreign interference can take a myriad of forms, including disinformation campaigns on social media to shape public opinion, cyber-attacks targeting critical infrastructure related to elections, and direct and indirect financial support of political actors.* [6]

Nevertheless, the above list cannot replace the need for a uniform definition. Echoing the words of Kristine Berzina and Etienne Soula in *Conceptualizing Foreign Interference in Europe*, 'inconsistency in language could complicate policymaker and public understanding of what interference is'.[7] According to their review of the concept, foreign interference has two core elements: malicious intent and lack of transparency. As for the former**,** the authors suggest looking at the final aim behind the operation. More specifically, actors that legitimately seek to exercise a form of benign influence on the behaviour of other states in the pursuit of their own interests – i.e. soft power and public diplomacy – should not count as foreign interferences.[8] On the contrary, practices that are meant to 'disrupt, manipulate, damage or erode confidence in democratic organizations, institutions and processes' warrant the

[2] von der Leyen, U. *A Union that Strives for More. My agenda for Europe. Political Guidelines for the Next European Commission 2019-2024*, Brussels, 2019.

[3] Council of the European Union, *Complementary efforts to enhance resilience and counter hybrid threats - Council Conclusions*, 14972/19, Brussels, 10 December 2019.

[4] European Parliament, *Resolution of 10 October 2019 on foreign electoral interference and disinformation in national and European democratic processes*, P9_TA(2019)0031, Brussels, 10 October 2019.

[5] European Parliament, *Foreign influence operations in the EU*, PE 625.123, Brussels, July 2018.

[6] European Parliament, *Resolution of 10 October 2019 on foreign electoral interference and disinformation in national and European democratic processes*, Cit.

[7] Berzina, K. and Soula, E., *Conceptualizing Foreign Interference in Europe*, Alliance for Securing Democracy, 18 March 2020, p. 3.

[8] Soft power is defined as 'the ability to affect others to obtain the outcomes one wants through attraction rather than coercion or payment', while public diplomacy essentially refers to 'means of promoting a country's soft power', according to Nye, J.S., *Public Diplomacy and Soft Power*, The Annals of The American Academy, No. 616, March 2008. For further information, see Melissen, J., *The New Public Diplomacy. Soft Power in International Relations*, Palgrave MacMillan, New York, 2005.

label.[9] Malevolence should be assessed on the basis of 'timing, coordination between actors and scale of effect'.[10]

With respect to the second element, they highlight the opaque nature of these operations. Indeed, foreign actors actively try to hide their efforts and the methods employed to intentionally disrupt other countries. This is true both for information strategies and illegal financial and political funding. Regarding the 'foreign' connotation, it should be noted that interferences are not always, necessarily, external: of course, domestic actors can maliciously undertake operations intended to destabilize their own political system. However, this chapter will only focus on the threat posed by external actors to other countries and the EU – although these same practices may foster the aims of some national actors.[11]

The operationalization of the concept, or the practical side of it, is based on the idea that foreign interferences can assume different forms and therefore promote 'hybrid' political and military strategies. The notion of hybrid threat is not a rigid one because of its evolving nature;[12] however, some features appear constantly. As expressed in a Joint Communication of the Commission and the HR to the EP and the Council:

> *'The concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare*[13]

Foreign interferences fit perfectly in this category. In fact, they involve a series of different operations that lay in this 'grey zone' between war and peace, including cybercrime, malicious and/or illegal financial activity, economic coercion, and information operations.[14]

Cybercrime mainly includes two types of operation. The more traditional 'cyber-enabled crimes' refer to crimes whose scale and reach is enhanced using computers, such as fraud, xenophobia, identity theft and sexual abuse. 'Cyber-dependent crime', instead, includes any crime that can only be committed using computers, for example illegal interference with computer data or systems, illegal access of computer data, computer misuse tools like malware, hacking and Distributed Denial of Service (DDoS) attacks.[15]

---

[9] Berzina, K. and Soula, E., Cit., p. 4.

[10] *Ibidem*, p. 10.

[11] Decker, B., *Adversarial Narratives: A New Model for Disinformation*, Global Disinformation Index, August 2019, p. 11; EUvsDisinfo, *Methods of Foreign Electoral Interference*, 2 April 2019. https://euvsdisinfo.eu/methods-of-foreign-electoral-interference/

[12] There is an ongoing debate among scholars about the terms 'hybrid warfare' and 'hybrid threat', since this form of conflict is located in the grey zone between war and peace, falling short of using military tools. See Hoffman, F. G., *Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict*, Institute for National Strategic Studies National Defense University, No. 240, April 2009; Giumelli, F., Cusumano, E. and M. Besana, *From Strategic Communication to Sanctions: The European Union's Approach to Hybrid Threats*. In E. Cusumano and M. Corbe (eds), *A Civil-Military Response to Hybrid Threats*. Springer International Publishing, 2018.

[13] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council. Joint Framework on Countering Hybrid Threats. A European Union response*. JOIN(2016) 18 final, Brussels, 6 April 2016.

[14] Berzina, K., Kovalcikova, N., Salvo, D. and Soula, E., *European Policy Blueprint For Countering Authoritarian Interference In Democracies*, Alliance for Securing Democracy, No. 18, Washington D.C., 3 July 2019.

[15] DDoS are aimed to disrupt networks' traffic by attacking the target with overwhelming Internet traffic. For further information, see McGuire, M. and Dowling, S., *Cyber-crime: A review of the evidence*, Home Office, Research Report 75, Chapter 1 and 2, London, October 2013.

Malicious or illegal financial activity includes covert financial support to political parties or organizations, as well as pure financial crimes, which 'range from basic theft or fraud committed by ill-intentioned individuals to large-scale operations masterminded by organized criminals with a foot on every continent'.[16] This is different from strategic economic coercion, which stands for the "efforts at coercive or threatening economic behaviour by an initiating government directed against a target government", and includes 'the deliberate disruption, or threat of disruption, of customary trade, financial, or other economic relations'.[17]

Finally, particular attention should be given to information operations.[18] The first type is misinformation, or the sharing of false information which is not linked to a malicious intent to cause harm, although it actually does so.[19] The second is disinformation, or the intentional sharing of false information to inflict harm.[20] The third is mal-information, or the sharing of genuine information to cause harm, and may consist in leaks, harassment and hate speech.[21] They usually target a specific audience with specific socioeconomic and political profiles and are spread in different formats through digital platforms, advertising tools, automated accounts – or 'bots' - and individuals.[22] These terms are preferred to more politicized and mediatic ones, such as 'fake news', which is often used interchangeably with disinformation, but is still inadequate in describing the complex phenomenon of information operations.[23] Finally, this phenomenon is often linked to the notion of propaganda, which is intended as the art of influencing and manipulating ideas and behaviours in order to "mislead a population, as well as to interfere with the public's right to know and the right of individuals to seek and receive, as well as to impart, information and ideas of all kinds."[24] In what follows, the notion of 'disinformation' includes these three different elements.

Democracies are the main targets of foreign interference operations. In fact, the openness of the democratic model, combined with the intrinsic vulnerability of new technologies, enables foreign actors to easily interfere in the economic, social, and political space.[25] In particular, cybercrime can damage sensitive national infrastructures, as well as citizens' online data, identities and personal affairs.[26] It can also target electoral infrastructures and delegitimize the election result, as was attempted in the case of the US 2016 presidential elections.[27] Economic coercion gives foreign actors

[16] Interpol, *Financial Crime.* https://www.interpol.int/Crimes/Financial-crime

[17] Tanner, M., *Economic Coercion: Factors Affecting Success and Failure. In Chinese Economic Coercion Against Taiwan: A Tricky Weapon to Use*, Rand Corporation, Santa Monica, 2017, pp. 11-32.

[18] Cf. European Parliament. *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*. Policy Department for Citizens' Rights and Constitutional Affairs. PE 608.864. February 2019.

[19] Reid, A., Waldman, A., *Viral 'Rigged' Voting Machine Video Actually User Error*, Electionland, 8 November 2016; Rogers, K., Bromwich, J. E., *The Hoaxes, Fake News and Misinformation We Saw on Election Day*, New York Times, New York, 11 September 2016.

[20] Council of Europe, *Information disorder: Toward an interdisciplinary framework*, Council of Europe Report DGI(2017)09, Strasbourg, 17 September 2017, p. 21.

[21] Smith, D., *WikiLeaks emails: what they revealed about the Clinton campaign's mechanics*, The Guardian, 6 November 2016.

[22] European Parliament. *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*. Cit., pp. 30-35.

[23] *Ibidem*, p. 25.

[24] *Ibidem*, p. 27.

[25] Kello, L., *The Virtual Weapon and International Order*, Yale University Press, New Haven, 2017. The Council of the EU has identified in 'manipulation using online technologies including disinformation campaigns' one of the key challenges to democracy. See Council of the EU, *Council Conclusions on Democracy*, Brussels, 14 October 2019.

[26] Rugge, F., *Cybercrime and international relations*, Istituto per gli Studi di Politica Internazionale (ISPI), 16 July 2018.

[27] U.S. Department of Justice, Mueller, R. S., *Report on The Investigation into Russian Interference in The 2016 Presidential Election*, Washington D.C., March 2019.

the possibility to gain leverage over governments and threaten policy-making autonomy.[28] Malicious financial activity in the market prevents economies from functioning properly, while external funding to political parties may damage fair competition and autonomy to the advantage of third actors (cf. Chapter 5).[29]

False or misleading information distorts the views of individual citizens and threatens their ability to take conscious political decisions, thus affecting policy and election outcomes. According to Tucker *et al.* (2018),[30] these operations can impose some narratives that positively, negatively or inflammatorily frame particular topics and therefore polarize public opinion. Polarization, in turn, can undermine the quality of public debate and respect for social norms as well as discourage parties from compromising. This phenomenon threatens the good functioning of participatory democracy, which requires 'the provision of information and effective processes of consultation'.[31] Moreover, election or referendum results that are directly hacked or indirectly manipulated through disinformation campaigns lose legitimacy and increase citizens' mistrust of institutions.[32] It also has a direct negative impact on human rights such as human dignity – including privacy and data protection - freedom of expression and right to information.[33] This topic has gained further relevance in recent times, when the COVID-19 emergency pushed for an intense use of online platforms and exposed citizens to serious disinformation operations (cf. Chapter 4).[34] To capture a state of affairs in which, through the extensive use of social media and networks, the boundaries between truth and lies become tenuous, the expression "post-truth politics" has become extensively used.[35]

1.3 Who sponsors foreign interferences?

There is plenty of research and empirical evidence showing that foreign interferences are a significant challenge for democracies. Due to their characteristics, methods, and aims, it is observed that these operations are usually carried out by autocratic countries. Although Russia remains the main state actor to consider, there are other emerging countries in this field, including China, Iran, and North Korea.

China, together with Russia, has conducted the main interference operations in liberal democracies. According to the 2018 report published by the Mercator Institute for China Studies,[36] in recent years the country has significantly invested in foreign operations deployed through political and economic elites, media, civil society, and academia. Although Chinese officials claimed that these operations constituted a part of economic and cultural cooperation, the line between 'influence' and 'interference'

[28] Tanner, *Economic Coercion: Factors Affecting Success and Failure. In Chinese Economic Coercion Against Taiwan: A Tricky Weapon to Use*, Cit., pp. 11-32.
[29] Kergueno, R., *Fraud and boats: funding European political parties*, Transparency International EU, 9 November 2017.
[30] Tucker, J. A., Guess, A., Barberá, P., Vaccari, C., Siegel, A., Sanovich Stukal, S. and Nyhan, B., *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*, Hewlett Foundatio, March 2018, p. 51.
[31] European Parliament, *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*, Cit., p. 62.
[32] *Ibidem*, p. 62. See also Ohlin, J. D., *Election Interference. International Law and the Future of Democracy*, Cambridge University Press, Cambridge, June 2020.
[33] *Ibidem*, pp. 73-79.
[34] Council of Europe, *LIBE exchange of views on disinformation in COVID-19 time*, Press release, Strasbourg, 12 May 2020.
[35] Giusti, S. and E. Piras, 'In Search of Paradigms: Disinformation, Fake News, and Post-Truth Politics'. in Giusti S. and E. Piras (Eds), *Democracy Under Attack? Disinformation, Fake News, and Post-Truth Politics*, London, Routledge, forthcoming.
[36] Benner, T., Gaspers, J., Ohlberg, M., Poggetti, L. and Shi-Kupfer, K., *Authoritarian Advance: Responding to China's Growing Political Influence in Europe*, *Global Public Policy Institute and Mercator Institute for China Studies*, February 2018. See also European Parliament, Foreign influence operations in the EU, Cit.

is often thin.[37] Indeed, China mainly aims at securing its regime stability and promoting its political and economic model as a viable alternative to the democratic model. To do this, Chinese leaders foster solid networks with European elites and seek to exploit existing divisions among EU countries.[38]

Iran and North Korea are two other emerging actors. Iran has made use of energy policy as a tool of foreign policy to gain leverage over its political adversaries, especially during the COVID-19 pandemic (cf. Chapter 4).[39] Moreover, Iranian leaders have begun to employ social media to polarize and target societies, especially the US.[40] As for North Korea, there is a growing consensus that considers it as a new cyber-power, especially for its hacking capabilities;[41] in addition, the country is progressively merging cyber tactics with information operations at the expense of Western countries.[42]

1.3.1 Russia and its hybrid strategy

Despite a growing number of new actors involved in the field, Russia remains the main threat for the EU because of its geographic position and the scale of its operations. Its tactics perfectly fit in the category of hybrid threat and foreign interference. This is particularly true if one considers the imbalances in the relationship between Russia and the West. Notwithstanding the grandiose ambitions of President Vladimir Putin to restore Russia's 'Great Power' status, serious problems persist.[43] In fact, if 'Great Power' status is measured on the basis of military capability, economic resources and cultural and political attractiveness, Russia lags behind on all standards, to various extents.[44] In relation to military capabilities, Russia remains one of the major (nuclear) powers, though not fully modernized *vis-à-vis* the US.[45] As regards its economy, Russia's GDP remains relatively low and is not expected to increase significantly over the next few years.[46] Concerning the systems' attractiveness and soft power, Russia presents significant deficiencies.[47]

Being conscious of this quite unbalanced relationship, General Valery Gerasimov, Chief of the General Staff of the Armed Forces, has developed a comprehensive hybrid strategy which aims at weakening competing countries in the global arena using non-military means. In *The Value of Science Is in the*

---

[37] European Parliament, *China's foreign influence operations in Western liberal democracies: An emerging* debate, At A Glance, PE 621.875, Brussels, May 2018; European Parliament, *China's Maritime Silk Road initiative increasingly touches the EU*, Briefing, PE 614.767, Brussels, March 2018 ; See also McBride, J. and Chatzky, A., *Is 'Made in China 2025' a Threat to Global Trade?*, Council on foreign Relations, 13 May 2019.; Kurlantzick, J., *As China Extends Its Reach Abroad, When Does Influence Become Interference?*, World Politics Review, 8 January 2018.; Svárovský, M., Janda, J., Víchová, V., Gurney, J. and Kröger, S., *Handbook On Countering Russian And Chinese Interference In Europe*, European Values Center For Security Policy, 2019; Bond, D. and Fildes, N., *UK Intelligence Panel Warns on Huawei Security Flaws*, Financial Times, 28 March 2019.

[38] European Parliament, *China, the 16+1 format and the EU*, PE 625.173, Brussels, September 2018. See also Rühlig, T. N., Jerdén, B., van der Putten, F., Seaman, J., Otero-Iglesias, M., Ekman, A., *Political values in Europe-China relations*, European Think-tank Network on China (ETNC) Report, December 2018.

[39] European Parliament, Foreign influence operations in the EU, Cit., p. 5; Faucon, B., *Iran Leverages Oil to Court Other U.S. Rivals During Pandemic*, The Wall Street Journal, 11 May 2020.

[40] Hanon, B., *Iran's Newest Info Op Shows an Evolution of Tactics*, Alliance for Securing Democracy, 13 November 2018.

[41] Sanger, D. E, Kirkpatrick, D. D. and Perlroth, N., *The World Once Laughed at North Korean Cyberpower. No More*, New York Times, 15 October 2017; Crawford, A., *Assessing North Korea's Cyber Evolution*, Divergent Options, 25 November 2019.

[42] Ha, M., *North Korea Turns to Cyber Disinformation Attacks Amid Global Coronavirus Outbreak*, Foundation for Defense of Democracies, 1 April 2020

[43] Frye, T., *Putin touts Russia as a great power. But he's made it a weak one*, Washington Post, 6 June 2019.

[44] Klein, M., *Russia's Military Capabilities*, Stiftung Wissenschaft und Politik, Research Paper 2009/RP 12, October 2009, p. 8.

[45] Global Firepower, *Russia Military Strength*, 2020.

[46] Efremov, S., *The Challenges of Russia's Economy: An Overview*, Istituto per gli Studi di Politica Internazionale, 4 November 2019.

[47] Mcclory, J., *The Soft Power 30. A Global Renking of Soft Power*, Portland, 2018.

Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations (2013), he stated that:

> *Rules of war have changed significantly, use of non-military means to achieve political and strategic goals has increased in such a manner that it has exceeded the use of weapons in some cases. Methods used in struggles are political, economic, information-related, humanitarian, and other non-military means which are used by utilizing the population's potential for protest. Goals will be achieved by using clandestine military operations, information confrontation, and special operations*[48]

He also added:

> *No matter what forces the enemy has, no matter how well-developed his forces and means of armed conflict may be, forms and methods for overcoming them can be found. He will always have vulnerabilities and that means that adequate means of opposing him exist.*[49]

It is therefore clear that Russian elites have looked for unconventional methods to overcome asymmetries of power. To do so, all means covered by the notion of 'foreign interference' are valid, including the newest methods made possible by contemporary technological developments, but also economic and energy coercion and illegal financing.[50]

In particular, the Kremlin has invested significant resources in information operations. It is important to underline that Russian information warfare is not new, but has evolved by adapting to the new cyber-space, and is currently the main pillar of the Russian hybrid strategy.[51] It merges different operational fields and includes malicious influence on Western media; DDoS attacks that block the functioning of entire infrastructures through targeting malwares; paralysation of journalism with threat of libel; confusion and disorientation of the West with mixed messaging and disinformation campaigns through social media; polarization and division of public opinion on sensitive topics, such as immigration and gender orientation; illegal political party funding and buying up of political influence.[52]

Several practical examples of Russian foreign interference strategy can be made. The case of the 2016 US presidential elections stands out. Although there is no certainty about the fact that Russian political leaders themselves had a direct link with this operation, it is nonetheless true that the foreign actors involved had clear links with Russia.[53] As Lucas Kello wrote in *The Virtual Weapon and International Order*,[54] the interference was a clear example of "cyber exploitation", or 'penetration of an adversary's computer system for the purpose of exfiltrating data'.[55] In practice, it involved the Russian tactic of *kompromat*, that is 'the release of sensitive information about a public official in order to inflict reputational harm and alter the current political process'.[56] In fact, during the presidential race, the multi-national media organization WikiLeaks published twenty thousand email records that damaged

[48] Gerasimov, V., *The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations*, trans. Robert Coalson, Military-Industrial Kurier, 27 February 2013.
[49] Galeotti, M., *The 'Gerasimov Doctrine' and Russian Non-Linear War*, Moscow's Shadows, 2014.
[50] Karlsen, G. H., *Divide and rule: ten lessons about Russian political influence activities in Europe*, Palgrave, 8 February 2019.
[51] Snegovaya, M., *Putin's Information Warfare in Ukraine. Soviet Origins of Russia's Hybrid Warfare*, Institute for the Study of War, Russia Report I, Washington, September 2015.
[52] Pomerantsev, P. and Weiss, M., *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, Institute of Modern Russia, New York, 2014.
[53] Shane, S. and Mazzetti, M., *The Plot to Subvert an Election*, The New York Times, 20 September 2018.
[54] Kello, *The Virtual Weapon and International Order*, Cit.
[55] *Ibidem*, p. 53.
[56] *Ibidem.*

Hillary Clinton's public image. According to American intelligence, the attack was conducted by APT-28, a Russian hacking group linked to GRU, the Russian military intelligence.[57] Later, it was discovered that social networks were also used to support one candidate rather than the other and promote disinformation campaigns. Finally, experts at the Department of Homeland Security (DHS) found that Russian hackers tried to manipulate the voting machines in twenty-one states, even if there is no evidence that they managed to affect the vote counts.[58]

In the case of Ukraine, Russia has employed the technique of 'reflexive control' since 2014 to persuade the West not to hinder its efforts to disrupt the country.[59] The strategy is based on the use of information operations to "cause a stronger adversary voluntarily to choose the actions most advantageous to Russian objectives by shaping the adversary's perceptions of the situation decisively."[60] Russian leaders deeply shaped the narrative about Russian actions in Ukraine both through traditional and social media, with mixed results. On the one hand, this strategy undermined cohesion within NATO; on the other hand, it failed to change public attitudes towards Russia's actions in Ukraine.

Moving to EU countries, in 2007 Estonia was hit by cyber-attacks targeting sensitive infrastructures such as public institutions, banks, and small businesses. Although the Russian government denied its direct involvement, the malware used had a Russian-language origin and the attacks coincided with a period of civil disturbance between Estonia and Russia. These events caused major economic and political problems, but the country showed resilience to the attacks.[61]

More generally, as the empirical chapters of this report show, Russia has frequently interfered with other EU countries through disinformation campaigns, especially in critical times such as the COVID-19 emergency, attempting to distort elections and referenda, and financing 'friendly' political parties.

1.4 The way forward: responding to the challenge

This Chapter has introduced the concept of 'foreign interference' characterised, as in the most recent literature, by the core elements of malicious intent and lack of transparency. A variety of hybrid threats are therefore characteristic of foreign interference: from cybercrime to election manipulation, from the financing of political parties to energy disruptions, from economic coercion to information operations. Autocratic state and non-state actors are increasingly employing such threats against Western democracies, which are attacked through their structural elements of vulnerability, such as their openness.

Despite new emerging countries like China, Iran and North Korea employing such hybrid tactics, Russia is still the most relevant player in the field. Empirical evidence of its *modus operandi* is provided by the cases of the 2016 U.S. elections, Ukraine in 2014 and Estonia in 2007. Hit by Russia's aggressive behaviour and actions, governments have responded by setting up new strategies and instruments that seek to tackle it effectively.

The US, for instance, established the Cybersecurity and Infrastructure Security Agency (CISA) in 2018 with the aim of 'combatting cyber-crime and cyber incident response securing federal networks, protecting critical infrastructure, and providing cybersecurity governance, promoting information

[57] Beauchamp, Z., *The key findings from the US intelligence report on the Russia hack, decoded*, Vox, 6 January 2017.
[58] Shane and Mazzetti, *The Plot to Subvert an Election*, Cit.
[59] Snegovaya, *Putin's Information Warfare In Ukraine. Soviet Origins Of Russia's Hybrid Warfare*, Cit.
[60] *Ibidem*, p. 7.
[61] NATO StratCom, *Hybrid Threats: 2007 cyber-attacks on Estonia*, NATO StratCom, 6 June 2019.

sharing, training and exercises, and cyber safety information'.[62] In January 2017, the DHS had designated election infrastructure as 'critical infrastructure', and the Agency was then tasked to provide services like vulnerability assessments, malware analysis, information sharing and staff training. The COVID-19 crisis has provided an additional challenge in view of the 2020 presidential elections: supplementary resources and efforts are therefore being made by CISA, as well as federal and industry partners, to enhance infrastructure.[63]

Foreign interferences and hybrid threats sow confusion among citizens, polarise debate in public opinion and erode trust in public institutions and their actions. All in all, they represent a major threat to democratic governance. Tackling them is a complex endeavour, requiring differentiated responses and involving several actors and institutions at the local, national and international levels. This report maps and provides a preliminary assessment of the responses to foreign interferences set up and implemented by the EU (Chapter 2). The success (or lack thereof) of its action to minimise foreign electoral interference ahead of the 2019 EP elections and the impact of disinformation in the covid-19 crisis will be assessed in Chapters 3 and 4, while the issue of party financing will be covered by Chapter 5. Finally, taking stock of the evidence presented in the empirical chapters of this report, Chapter 6 provides specific policy recommendations.

[62] U.S. Department of Homeland Security, *Cybersecurity*. https://www.dhs.gov/topic/cybersecurity
[63] CISA, *Election Security*. https://www.cisa.gov/covid-19-and-elections

2. FOREIGN INTERFERENCES AND THE EU'S RESPONSES

KEY FINDINGS

- The EU has developed a comprehensive and multidimensional approach to tackle 'hybrid threats', defined as a 'mixture of conventional and unconventional, military and non-military, overt and covert actions falling below the threshold of formally declared warfare';
- While responsibility for detecting, preventing and responding to hybrid threats remains at the national level, EU action complements and strengthens national level responses. Coordination with and among national authorities has recently been reinforced, as has cooperation with NATO;
- Disinformation campaigns waged by Russia, China and other state and non-state actors, often via online platforms and social media, led the Commission to propose a Code of Practice on Disinformation, a self-regulatory instrument to counter online disinformation;
- The EU has paid increasing attention to strategic communication, setting up three Task Forces within the EEAS with the objective of improving the outreach and external image of the EU while, at the same time, refuting 'fake news';
- The European Parliament has pushed strongly for more assertive action by the EU to tackle foreign interferences and disinformation, particularly in the run-up to elections. It calls for sustained effort and action at the EU and national level.

2.1. Introduction

This chapter explores the EU's institutional responses to the challenge of foreign interferences. In particular since 2015 – following Russia's annexation of Crimea – the EU has significantly stepped up its efforts to counter foreign interferences. It should be noted that the action of the EU complements that of its MS. Detecting, preventing and responding to such threats remains primarily a national responsibility, supported and enhanced by actions at the EU level.

From 2016 onwards, the EU has employed the concept of 'hybridity' to capture the wide range of destabilisation tools and unconventional threats that fall under the threshold of military force. Foreign interferences may take several different forms (Cf. Chapter 1): from disinformation to cyber-attacks, from disruption of energy supplies to the overt or covert financing of political parties. Given the broad catalogue of hybrid threats, often sponsored by foreign actors, the EU has embraced a comprehensive approach and has set up a wide array of responses to tackle them.

This chapter describes the institutional responses – the strategies, positions and tools – developed by the EU to effectively tackle malicious activities by foreign players, both state and non-state actors. The ensuing chapters will, instead, focus on specific events – such as the 2019 EP elections and the coronavirus crisis – or actors – such as political parties – to empirically assess the actions put in place by the Union and its MS.

The rest of this chapter will develop as follows. Section 2.2 discusses the concept of hybrid threat and looks at the actions undertaken by the EU. Section 2.3 describes EU actions against disinformation, while section 2.4 presents the Strategic Communication Task Forces. Section 2.5 focuses on the strategic cooperation between the EU and NATO. Finally, section 2.6 discusses the current and future agenda of the EU in the fight against foreign interferences and, in particular, disinformation.

2.2. Hybrid threats and hybrid warfare

The concept of 'hybrid threat' is used to capture a grey area in which the distinction between peacetime and wartime is blurred. Such threats may combine military and non-military tools, conventional and non-conventional means and target society at large - for instance, through large-scale disinformation campaigns. Give their nature, hybrid threats cannot be countered solely by military means but require an equally inclusive – or, using the EU's jargon, 'comprehensive' – response encompassing different civil and military, public and private institutions and actors.[64] The list of hybrid activities is a long one, and includes, among others, cyber operations, forms of economic warfare, energy disruptions, and information operations.

While hybrid threats do appear similar to more traditional threats – having been employed for a long time by states and non-state actors alike, in the form of propaganda or espionage – a key difference between the latter and today's hybrid threats is the changing technological environment, which makes them 'far more deadly […] The internet and online networks allow state and non-state actors to unleash their aggression in new ways'.[65]

The aggressive behaviour of Russia in the EU Eastern area and, particularly, the war in Ukraine in 2014 pushed the EU to take more resolute action. The activities of Daesh/ISIL in itsSouthern neighbourhood and cyberattacks from places like China and Iran further triggered the EU's responses. In March 2015 the European Council urged a swift response to tackle Russian disinformation activities, while the concept of hybrid threat was explicitly developed at a later date, in the Joint Framework on Countering Hybrid Threats – a European Union Response, presented by the European Commission and the HR on 6 April 2016.

The Joint Framework defines hybrid threats as a 'mixture of conventional and unconventional, military and non-military, overt and covert actions that can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare'. Employing a wide array of tools and measures, hybrid threats have a shared objective, that is, 'to undermining public trust in government institutions or exploiting social vulnerabilities'. The Joint Framework brings together existing EU policies into a comprehensive approach aimed at fostering the resilience of the EU while increasing cooperation with NATO.[66]

This important document set forth 22 operational actions spanning from cybersecurity to disinformation, from counter terrorism to energy policy, involving a wide array of institutions and actors, encompassing both the EU and the national level. Notwithstanding its breadth, the progress

[64] Cusumano E. and M. Corbe (eds), *A Civil-Military Response to Hybrid Threats*, Springer International Publishing, 2017, p.2. NATO defined hybrid threats as 'those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives'. Cf. NATO, *BI-SC Input for a new NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*. 25 August 2010.

[65] Fiott, D. and R. Parkes, *Protecting Europe. The EU's response to hybrid threats*, European Union Institute for Security Studies, Chaillot papers / 151, April 2019, p. 5.

[66] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament and the Council. Joint Framework on Countering Hybrid Threats. A European Union response*. JOIN(2016) 18 final, Brussels, 6 April 2016.

reports published in 2017 and 2018 noted the overall 'good progress' made in the implementation of the actions.[67] Among them, it is worth mentioning the creation of the EU Hybrid Fusion Cell inside the EU INTCEN in 2017, which aimed to raise situational awareness and provide strategic analyses to EU decision-makers. The Joint Framework was followed by a Joint Staff Document providing the operational protocol to counter hybrid threats.[68]

In other strategic documents issued at around that time the concept of hybrid threat was further elucidated. This is the case with the 2016 Global Strategy, in which hybrid threats were identified as a key challenge to EU security.[69] The concept of hybrid threat was further used in the November 2017 Joint Communication - A Strategic Approach to Resilience in the EU's External Action.[70] In March 2018, the European Council, responding to the poisoning of a Russian agent and his daughter in the English town of Salisbury, urged the EU and the MS to continue to 'bolster their capabilities to address hybrid threats, including in the areas of cyber, strategic communication and counter-intelligence'.[71]

In June 2018 the Commission and the HR issued a Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats, which identified areas where action should be intensified, such as improving the capacity to detect hybrid threats, actions against chemical, biological, radiological and nuclear threats, strategic communication and disinformation, deterrence in the cybersecurity sector and resilience to hostile intelligence activity.[72]

Hybrid threats remained a very high priority in the EU agenda during 2019, with the particular activism of the Finnish Presidency of the Council of the EU in the second half of 2019. In its work programme, the Finnish Presidency committed itself to placing 'special emphasis on strengthening the EU's capabilities in countering hybrid threats and building resilience' and to further developing 'institutional mechanisms and tools'.[73] Due to its impulse, and building on the work of the previous Presidency (Romania), a permanent horizontal working party of the Council was created in July 2019 to coordinateactivities aimed at countering hybrid threats, including disinformation campaigns.[74] An important objective, that is, to 'enhance the resilience and improve the security culture of the EU against cyber and hybrid threats from outside the EU' was further underscored, at the highest level, by the European Council.[75]

---

[67] See European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats – a European Union response*, JOIN(2017) 30 final, Brussels, 19 July 2017 and European Commission,. *Joint report to the European Parliament, the European Council and the Council on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018*. JOIN(2018) 14 final. Brussels, 13 June 2018.

[68] European Commission, High Representative of the Union for Foreign Affairs and Security Policy,. *Joint Staff Working Document. EU operational protocol for countering hybrid threats. 'EU playbook'*, SWD(2016) 227 final, Brussels, 5 July 2016.

[69] European External Action Service, *Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy*, 28 June 2016. See also Sperling, J., 'The European Union and the grand security strategy for post-Westphalian governance', *EU Security Strategies. Extending the EU System of Security Governance*. Routledge, 2018, pp. 11-12.

[70] European Commission, *Joint Communication to the European Parliament and the Council - A Strategic Approach to Resilience in the EU's external action*, JOIN(2017) 21 final, Brussels, 7 June 2017.

[71] European Council, *Conclusions*, Brussels, 23 March 2018.

[72] European Commission, *Joint communication to the European Parliament, the European Council and the Council - Increasing resilience and bolstering capabilities to address hybrid threats*, Join(2018) 16 final, Brussels, 13 June 2018.

[73] Finland's Presidency Programme, *Sustainable Europe – Sustainable Future*, Presidency of the Council of the EU, 1 July – 31 December 2019.

[74] Council of the European Union, *Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats – Establishment and adoption of its Terms of Reference*, Brussels, 8 July 2019.

[75] European Council, *Conclusions*, Brussels, 20 June 2019.

2.3. Fighting disinformation

With the Russo-Ukrainian crisis and the ensuing EU sanctions, Russia stepped up its propaganda machinery and the anti-EU messages, targeting in particular, but not only, the EU's Eastern countries. To counter (mainly Russian) disinformation activities, defined as 'verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm[76] the EU took action to strengthen its strategic communication and tighten its policies and regulations.

In March 2015 the European Council, stressing the need to fight the ongoing Russian disinformation campaigns, tasked the HR to prepare an Action Plan on Strategic Communication by June.[77] This plan aimed to improve the external image of the EU while, at the same time, refuting 'fake news'. As argued by Giumelli and colleagues,[78] the overall ambition of the plan was defensive – i.e. discrediting false narratives rather than engaging in counter-propaganda activities. The plan was centred on three main elements. First, the effective communication and promotion of EU policies and values vis-à-vis the Eastern neighbourhood; second, strengthening the overall media environment including independent media; third, increasing public awareness of disinformation activities by external actors, and improving the EU capacity to anticipate them and respond.[79]

The threat posed by the disinformation activities of Russia and other foreign countries was clearly identified by the resolution of the EP of 23 November 2016 on strategic communication to counteract anti-EU propaganda by third parties.[80] The resolution went beyond the concept of disinformation, to explicitly talk about 'information warfare' and 'modern hybrid warfare'. It identified several forms of disinformation spread through the traditional media, social networks, school programmes and political parties. To counter disinformation, the EP advocated more decisive and coherent action by the EU, including the reinforcement of a StratCom TF (cf. below). The EP pushed the European Commission to further act against disinformation in its resolution of 15 June 2017 on Online Platforms and the Digital Single Market.[81]

From mid-2017 onwards, the Commission developed its strategic responses to the disinformation threat, starting a public consultation in October on fake news and public disinformation and setting up, in November, a High-level Expert Group representing academia, online platforms, the media and civil society. The Expert Group produced a report – 'A multi-dimensional approach to disinformation' – which constituted the basis for the communication on online disinformation released by the Commission towards the end of April 2018.[82]

The Commission's communication set up an action plan and endorsed self-regulatory tools to counter online disinformation. It was then followed, in September 2018, by the Code of Practice on

---

[76] European Commission, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Tackling online disinformation: a European Approach, COM(2018) 236 final, Brussels, 26 April 2018.

[77] European Council, *Conclusions*, Brussels, 20 March 2015

[78] Giumelli, F., Cusumano, E. and M. Besana, 'From Strategic Communication to Sanctions: The European Union's Approach to Hybrid Threats', *A Civil-Military Response to Hybrid Threats*. Springer International Publishing, 2017, p. 153.

[79] European Union, *EU action plan on strategic communication*, Ares(2015)2608242, 22 June 2015.

[80] European Parliament, *Resolution on EU strategic communication to counteract EU propaganda by third parties*, P8_TA(2016)0441, 23 November 2016.

[81] European Parliament, *Resolution on Online platforms and the Digital Single Market*, P8_TA(2017)0272, 15 June 2017.

[82] High-level Expert Group on fake news and online disinformation, *A multidimensional approach to disinformation.* Luxembourg, European Commission, March 2018; European Commission, *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Tackling online disinformation: a European Approach*, cit.

Disinformation, a self-regulation of online social companies.[83] With the EP elections scheduled in May 2019 and several examples of electoral interference occurring at the national level,[84] the Commission structured a comprehensive and robust plan to prevent or, at least, reduce the risk of electoral interference and the spread of disinformation in the run-up to the EP elections.[85] A package of measures – on Free and Fair European Elections – was proposed in September 2018. Such wide-ranging measures were followed by the Joint Action Plan of the Commission and the HR against disinformation in December 2018, aiming to further build up capabilities and strengthen cooperation between MS and EU institutions.[86]

Such activism by the EU clearly shows that, as the EP elections got closer, foreign interferences were regarded as a key security threat. The responses of EU citizens also reflected widely shared preoccupations concerning the impact of disinformation. A special Eurobarometer survey on 'Democracy and elections', published in November 2018, asked European citizens whether, in the pre-election period at any level of government, they had been concerned about disinformation and misinformation on the internet.[87] A large majority of Europeans were very or somewhat concerned about disinformation (73%), with no EU member country falling below the 50% majority threshold. A slightly lower, but still high share of respondents (67%) were worried about the (mis)use of personal data for micro-targeting and political advertising, another issue that the Commission intended prioritising. By contrast, a significantly smaller majority (55%) was preoccupied with restrictions and censorship of political debates.[88]

The fight against disinformation – defined by the European Council, in December 2018, as an "acute and strategic challenge for our democratic systems" – requires a "determined response […] that is comprehensive, coordinated and well-resourced".[89] A key action in this regard was the implementation of the Joint Action Plan. In the run-up to the EP elections, the EU created a new coordination structure to exchange information between MS and the EU – the European cooperation network on elections, which held its inaugural meeting in January 2019 – and a new tool, the RAS, designed to facilitate the exchange of information on 'fake news' between the national and EU level. The RAS was part of a broader network including the EU hybrid fusion cell, INTCEN and the Commission's Emergency Response Coordination Centre. The European Council acknowledged the 'important work' undertaken during this period, but still called for 'continued and coordinated efforts to safeguard the Union's democratic systems'.[90]

In this challenging context, the Commission itself developed its daily media outreach and communication campaigns. The Commission's Representations in the MS were also expected to play a significant role against disinformation, given their privileged national vantage point. Furthermore,

[83] European Commission, *EU Code of Practice on Disinformation*, 26 September 2018.

[84] Cf. Brattberg, E. and T. Maurer, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, 23 May 2018.

[85] The detailed analysis of the EU responses to foreign interferences in the run-up to the 2019 EP elections is developed in Chapter 3.

[86] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Action Plan against Disinformation*, 5 December 2018.

[87] Special Eurobarometer 477, Wave EB 90.1. *Democracy and elections*, November 2018.

[88] The Special Eurobarometer, *Fake News and Disinformation Online*, published in April 2018 (fieldwork: February 2018), asked European citizens whether fake news represent a problem for democracy. 83% of respondents agreed with the statement, ranging from 89% in Cyprus to 74% in Estonia. Interestingly, national authorities were mentioned more frequently than the EU institutions when citizens were asked to identify the institutions which should act to stop "fake news".

[89] European Council, *Conclusions*, Brussels, 14 December 2018.

[90] European Council, *Conclusions*, Brussels, 22 March 2019.

dedicated resources were assigned across different services to detect disinformation, coordinate responses and, eventually, feed information into the RAS.

As Chapter 3 shows, an organised and systematic disinformation campaign did not affect the 2019 EP elections. Yet, the Heads further reiterated the need for 'sustained efforts to […] strengthen the resilience of our democracies to disinformation' in June 2019.[91] Indeed, the agenda of the European Commission led by Ursula von der Leyen placed a strong focus on fighting disinformation and tightening up the regulatory regime for social media platforms.

2.4. Strategic communication

To counter disinformation and the interferences from Russia, the EU reformed and strengthened its strategic communication. In March 2015, the Heads stated that the ongoing disinformation campaigns required a robust response from the EU and the creation of a communication team.

The Task Force – as it was then called – was eventually created in September 2015 under the EEAS. Its Strategic Communications Division became responsible for designing and leading communications and outreach activities in support of the EU's foreign policy objectives and the HR's activities. It was asked to play a leading role in tackling disinformation and addressing hybrid threats, particularly from foreign sources. Between 2015 and 2017, three TFs were established: first, the East StratCom TF in 2015, then TF South and the Western Balkans TF in 2017.

The East StratCom TF (https://euvsdisinfo.eu/) was designed with a specific geographical reach – the Eastern partnership region – and was in charge of developing communication products and campaigns to explain EU policies. It was also responsible for publishing a 'myth-busting', weekly Disinformation Review, involving a network of more than 400 experts, journalists, officials, NGOs and think-tanks in over 30 countries, which reported disinformation articles to EU officials, and the public. The Disinformation Review has not been spared from criticism due to its alleged lack of methodology and the fact that it does not ensure due process.[92]

The EP has vocally endorsed the strengthening of the EU's strategic communication. In its resolution of 23 November 2016, Strategic communication to counteract anti-EU propaganda by third parties, the EP not only commended the 'significant work' accomplished by the TF, but strongly pushed for its reinforcement and expressed its support for making it a fully-fledged unit within the EEAS, properly staffed and with the necessary budgetary resources, possibly enabled by a dedicated budget heading. The 2016 US presidential elections were a wake-up call for the EU on disinformation, and the EP has advocated a more effective communication strategy to the outside world on the merits of the EU's actions and policies.[93]

In the early years of its activity, the TF's limited resources – it did not have resources of its own and relied on the EEAS general budget for strategic communication – and its dependence on mostly seconded staff limited its effectiveness. Indeed, MS were also dissatisfied by this state of affairs – while facing more aggressive disinformation attacks from abroad and in particular from Russia – and, in an open letter, eight of them – the Czech Republic, Croatia, Latvia, Lithuania, Poland, Romania, Sweden and the UK – urged the EEAS to further enhance the StratCom TF. At the time, the East StratCom TF

[91] European Council, *Conclusions*, Brussels, 20 June 2019.

[92] European Parliament, *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*, Policy Department for Citizens Rights and Constitutional Affairs, PE 608.864, Brussels, February 2019, p. 98; Wagnsson C. and M. Hellman, Normative Power Europe Caving in? EU under Pressure of Russian Information Warfare, *Journal of Common Market Studies.* Vol 56, No 5, p. 1163.

[93] European Parliament, *Resolution on EU strategic communication to counteract EU propaganda by third parties*, Cit.

only had 14 members of staff, 10 of whom were seconded from national governments or other institutions, while the Western Balkans TF enlisted two and the TF South six additional seconded diplomats.[94]

This situation finally changed when an amendment of the EP to the 2018 budget included the 'StratCom Plus' pilot project, which gave the TF its first, real budget of €1.1 million, while €800.000 was allocated to the EEAS for strategic communication. The budget was significantly increased again in 2019 and it is now about €6 million. Recently, there has also been a notable increase in staff numbers, with 38 people currently working in the TF.[95] The EP has been a strong supporter of the TF, inviting – in its recommendation to the Council and the VP/HR of 13 March 2019 – all MS to second national experts and underscoring the need to equip the TF with new staff and skills, and to recruit additional data scientists and disinformation experts.[96]

Indeed, the progress made in terms of staff, budget and operational capacity has been welcomed in the 2019 HR Report on the implementation of the framework for countering hybrid threats. The report notes that significant progress has been made in 'strengthening cooperation between the Commission services and the EEAS to tackle disinformation from external and internal sources' and that 'the Strategic Communication Division of the EEAS, its three Task Forces and the Hybrid Fusion Cell have been strengthened with additional staff'.[97]

2.5. Cooperation between the EU and NATO

NATO devoted its attention to hybrid threats ahead of the EU. Already in the early 2000s, responding to a changing politico-strategic environment, it devised a framework to set up CoE to be better equipped to counter emerging security threats.[98] NATO adapted its organisation relatively quickly also in the field of strategic communication. A StratCom cell had already been created in 2007 as a consequence of the failure to gain public support in Afghanistan, while in the 2009 Summit in Strasbourg/Kehl the leaders of the Alliance stated that 'strategic communications are an integral part of our efforts to achieve the Alliance's political and military objectives'.[99] In July 2014, a StratCom CoE was established in Riga.

Cooperation between the EU and NATO was fuelled by the changing security environment, which required new policies and different strategies. The declaration at the Wales Summit in September 2014 recognised that 'Russia's aggressive actions against Ukraine have fundamentally challenged our vision

[94] Rettman, A., 'Mogherini urged to do more on Russian propaganda', *EUObserver*, 20 October 2017.

[95] *Gessant C.* M. 'Borrell rejette les allégations de modification d'un rapport sur la désinformation', à la suite de pressions chinoises', *Agence Europe*, Brussels, 30 April 2020; European External Action Service, *Questions and Answers about the East StratCom Task Force*, 05 December 2018.

[96] European Parliament, *Recommendation to the Council and the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy concerning taking stock of the follow-up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda against it by third parties (2018/2115(INI)*, P8_TA(2019)0187, 13 March 2019

[97] High Representative of the Union for Foreign Affairs and Security Policy, *Joint Staff Working Document. Report on the Implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats*, SWD(2019) 200 final, 28 May 2019.

[98] Corbe, M., 'A Collective Response to Destabilisation: The NATO Centres of Excellence'. *A Civil-Military Response to Hybrid Threats*. Springer International Publishing. 2017.

[99] NATO, *Strasbourg / Kehl Summit Declaration*, 4 April 2009.

of a Europe whole, free, and at peace. Growing instability […] as well as transnational and multi-dimensional threats, are also challenging our security'.[100]

EU-NATO cooperation against hybrid threats gained more prominence in EU strategic documents and was visible at the operational level. In July 2016, the Global Strategy for the EU's foreign and security policy stated that the EU would enhance its strategic communications efforts and 'step up its contribution to Europe's collective security, working closely with its partners, beginning with NATO'.[101] In July 2016, the EU and NATO issued a Joint Declaration, where they agreed on a roadmap for their enhanced cooperation to tackle the new challenges in the South and the East, such as hybrid threats, enhancing resilience, defence capacity building and cyber defence.[102] Asked about the relationship between the East Stratcom TF and NATO, HR and VP Federica Mogherini replied:

> [the TF] *maintains contact with the US Government and with the NATO Strategic Communications team in NATO headquarters and Strategic Communications Centre of Excellence in Riga, to keep each side informed about the other's activities, exchange information on trends in strategic communication in the Eastern Neighbourhood and attend seminars and conferences. Contact with NATO will continue to take place in the context of the newly adopted EEAS/Commission services framework to counter hybrid threats, which envisages increased cooperation.*[103]

Further cooperation was made possible by the decision in April 2017 to establish the European Centre for Countering Hybrid Threats (Hybrid CoE) in Helsinki. The Centre was jointly opened by 10 EU MS, Norway and the USA. It established close contacts with the EU Hybrid Fusion Cell, operational since May 2017. The latter had achieved a membership of 27 by the end of 2019 and, according to a Joint Staff Working Document, 'made impressive progress with a growing membership, consensus approved work programme and a fully functioning budget'.[104]

In December 2018, the Joint Declaration pushed cooperation between the EU and NATO further,[105] while the fourth progress report on the implementation of the common set of proposals endorsed by NATO and the EU Council in July 2019 noted that 'cooperation on countering hybrid threats continued at a steady pace'. More in detail, it noted positive development in the cooperation activities between the CoE and the EU structures countering hybrid threats. In the Hybrid CoE in Helsinki, for instance, "EU and NATO staff continued active interaction [including] in the area of strategic communications to counter disinformation". Cooperation also occurred between the EU Stratcom TF and NATO Stratcom CoE, on issues such as pro-Kremlin narratives, the impact of Kremlin media channels in the EU and beyond, plans for further intensified cooperation in the Eastern Partnership Countries and training.[106]

---

[100] Cited in Drent, M., Hendriks, R. and D. Zandee, *New Threats, New EU and NATO Responses*, Clingendael Report, Netherlands Institute of International Relations, July 2015, p. 24.

[101] European External Action Service, *Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy*, Cit.

[102] NATO, *EU-NATO Joint Declaration*, 8 July 2016.

[103] Parliamentary questions, Answer given by Vice-President Mogherini on behalf of the Commission, E-002156/2016, 23 June 2016.

[104] Joint Staff Working Document, *Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats*, Cit.

[105] President of the European Council, President of the European Commission, Secretary General of the North Atlantic Treaty Organisation, Joint Declaration on EU-NATO Cooperation, 10 July 2018.

[106] NATO, *Fourth progress report on the implementation of the common set of proposals endorsed by NATO and the EU Councils on 6 December 2016 and 5 December 2017*, 17 June 2019, p. 4. See also Giumelli, F., Cusumano, E. and M. Besana, *From Strategic Communication to Sanctions: The European Union's Approach to Hybrid Threats*, Cit., p. 154.

Annex 1 summarises the participation of the EU-27 MS in key NATO or EU/NATO structures countering hybrid threats.

2.6. The EU's agenda after the 2019 European elections

The importance of countering foreign interferences did not diminish after the 2019 EP elections. The newly designated President of the European Commission – Ursula von der Leyen – gave high salience to the issue in her first speech before the EP in July 2019. Presenting the strategic agenda of the Commission for the 2019-2024 mandate, she described the EU security challenges as 'diverse and unpredictable' and referred to several 'serious and acute" hybrid threats, requiring the EU to "step up its response and resilience'.[107]

In the field of cyber-security, for instance, to diminish the EU's dependency on foreign countries and make it better equipped to prevent cyber-attacks, she urged the EU "to achieve technological sovereignty in some critical technology areas". More explicitly, in the section of her strategic agenda dedicated to 'European democracy', the President-elect made a strong plea to strengthen the EU's capacity to protect itself from external interference. Specifically, she underscored the need for a 'joint approach' and 'common standards' to tackle issues such as 'disinformation and online hate messages'. In concrete terms, she promised to present a European Democracy Action Plan to address the threat of external intervention in European elections and to put forward legislative proposals ensuring greater transparency of paid political advertising and clearer rules on the financing of European political parties (cf. Chapter 5).[108] Such commitments were confirmed in the Work Programme of the new Commission of January 2020.[109]

The new agenda of the European Commission has been elucidated in some additional detail by Věra Jourová, VP for Values and Transparency. In her opening speech at the conference 'Disinfo Horizon: Responding to Future Threats', on 30 January 2020, Jourová was very outspoken on the challenges of disinformation and foreign interference for democracy. Her critical focus was on specific external actors – Russia and, to an increasing extent, China – and their interference tactics to weaken European democracy, understood – broadly – as both the EU and the national levels. She promised not to be indifferent 'when others attack us with manipulation and disinformation' and called for a more active stance of the EU with a key role for its strategic communication.[110]

The flagship initiative of the Commission in this area is the European Democracy Action Plan, expected by the end of 2020.[111] It endeavours to have a broader scope than fighting disinformation alone and also aims to strengthen the media sector; to make social media platforms more accountable; to reinforce the democratic process and, more generally, to create a digital ecosystem able to defend and promote democracy. In addition, VP Jourová indicated her willingness to further regulate social media platforms, pushing them to be 'more accountable and responsible', and political advertising, where 'clarity' and 'legal certainty' are lacking. Investments in education and media literacy are set to

[107] von der Leyen, U. *A Union that Strives for More. My agenda for Europe*. Political Guidelines for the Next European Commission 2019-2024, 2019, p. 19.
[108] Ibidem, pp. 13, 21.
[109] European Commission, *2020 Work Programme: An ambitious roadmap for a Union that strives for more*, COM (2020) 37 Final, 29 January 2020.
[110] Jourová, V., *Opening Speech of Vice-President Věra Jourová at the Conference "Disinfo Horizon: Responding to Future Threats"*, 29 January 2020.
[111] Responsible for the Democracy Action Plan are Věra Jourová, Commissioner and Vice-President for Values and Transparency and Didier Reynders, Commissioner for Justice. The High Representative and Vice-President Josep Borrell, in charge of the EEAS, is also consulted. See Meyer-Resende M., *Von der Leyen's Plans. What to expect from EU regulation on online threats to democracy discourse*, Briefing Paper 105. Democracy Reporting International, 2020, p. 2.

continue: the EU financed a European Digital Media Observatory (EDMO) with €2.5 million and put €60 million into the Creative Europe Programme.

Further investments worth €5.1 million overall – connected to the broader EU agenda to fight disinformation – went into a package to promote media freedom and pluralism and were announced in early March 2020. A first initiative aiming to provide protection for reporters and covering areas such as fact-finding, monitoring, advocacy, informing the public and raising EU awareness was funded with €1.4 million granted to a consortium led by the European Centre for Press and Media Freedom. A second project received €1.5 million in financial support to support cross-border investigative journalism and was led by the International Press Institute.[112]

Moreover, a communication on Shaping Europe's Digital Future was issued by the Commission in February 2020. Acknowledging once again the threat posed by malicious cyberactivity to European security and democracy, the communication endorsed a stronger plan of action to defend the EU from attempted manipulations of the information space, which most likely come in the form of targeted and coordinated disinformation campaigns.[113]

Anticipating the content of the European Democracy Action Plan, the Commission reiterated the need for greater transparency in the ways in which information is shared and managed on the internet and to support trustworthy quality media. The communication also paved the way for the Digital Services Act, defining new rules for the operation of the digital ecosystem, including political advertising and online disinformation.[114]

The newly elected European Commission has, therefore, placed the issue of foreign interference – in its various forms – among its key agenda priorities. Several actions, plans and legislative measures are expected in the last quarter of 2020, with consultations with stakeholders scheduled beforehand.

The EP has repeatedly pushed the EU to step up its efforts. In its October 2019 resolution on foreign electoral interference and disinformation in national and European democratic processes, the EP put forward its position on the actions that the EU would need to pursue to tackle this 'major challenge' and, particularly, albeit not exclusively, 'Russia's disinformation campaigns'.[115] In the topical debate of 27 November 2019, the EP discussed the issue of interference from other countries in democracies and elections again. The specific requests by the EP and the responses of the EU and/or national institutions (at the time of writing) are summarised in Annex 2.

2.7. Conclusions

This chapter has reviewed the key actions and policies of the EU to counter foreign interferences. The focus has been placed on hybrid threats and, specifically, disinformation. The EU strategic thinking on hybrid threats and strategic communication has developed quite significantly from 2015 – when the European Council put the issue on its agenda – to the present day. The EU has set up a dialogue with social media platforms, created coordination systems with MS to detect and monitor disinformation activities, stepped up its cooperation with NATO and strengthened its TF with autonomous financial resources and staff.

[112] European Commission, *Media Freedom Projects*, 2 March 2020.
[113] European Commission, *Communication: Shaping Europe's Digital Future*. 19 February 2020.
[114] Stolton, S., 'Media freedom and pluralism 'key' to Democracy Action Plan', *Euractiv*. 3 March 2020.
[115] European Parliament, *Resolution on Foreign electoral interference and disinformation in national and European democratic processes*, P9_TA(2019)0031, 10 October 2019.

As the agenda of the Commission led by Ursula von der Leyen shows, and as the European Council has often reiterated in its conclusions, the threat of foreign interferences remains a top priority for the EU. Indeed, the COVID-19 crisis has demonstrated in an unprecedented way how damaging the issue of externally sponsored disinformation can be, and the importance of timely and effective responses by the EU (cf. Chapter 4). The EU is certainly much better prepared to face hybrid activities and counter disinformation in 2020 than it was only a few years ago. Still, the call of the EP for further action, reform and investments in the area finds strong justification in the large-scale operations undertaken by countries like Russia or China.

3. FOREIGN INTERFERENCES AND THE 2019 EP ELECTIONS

KEY FINDINGS

- The EU institutional response to the challenge of foreign interference in the 2019 EP elections was broad, comprehensive and varied;
- The Code of Practice on Disinformation was a first-of-a-kind attempt to tackle one of the most important facets of disinformation, such as the role of social media and advertising companies;
- At the same time, the Code's self-regulatory approach has partly hampered its effectiveness, and a stronger regulatory approach may be needed;
- The cooperation networks on elections have fostered increased coordination at the national and European level, and across levels;
- The Rapid Alert System was set up to allow for an immediate response to typically quick disinformation "bursts", but was not used before the elections;
- The East StratCom Task Force has identified and debunked several disinformation instances of Russian origin, but has also raised some concerns regarding its transparency;
- The nature of information operations in the EP elections seemed to rely more on polarisation and less on the fabrication of false or misleading factual statements, making fact-checking alone insufficient to tackle the threat and reinforcing the need for platform regulation and media literacy projects and development.

3.1. Introduction

In the run-up to the 2019 European elections, the EU decided to build up its countermeasures against foreign interference after several notable cases sounded the alarm. The issue of electoral interference became relevant in 2016, in the aftermath of the Brexit referendum and the 2016 US presidential elections.[116] These cases drew attention to dangers of disinformation operations, foreign funding and election-related attacks; moreover, the role played by social media platforms proved to be especially influential in favouring such operations, in particular after the Cambridge Analytica scandal drew attention to the manipulation potential represented by users' data and micro-targeting practices.[117] Since then, the Russian government and its controlled entities, such as its Internet Research Agency (IRA) troll factory and the media outlets RT and Sputnik, have specifically been put under the spotlight.

While all types of foreign interference (see Chapter 1) can and do occur constantly, democratic societies' elections and referenda have proven to be particularly important moments when the rewards for trying to perform influence operations may be especially high. Disinformation operations in particular have been observed to spike when the ballot box approaches and public debate becomes increasingly polarised, although the foundations of such operations may often be laid in advance.[118] As

[116] Jackson, D., *Issue Brief: How disinformation impacts politics and publics*, National Endowment for Democracy, 2018.
[117] House of Commons (UK), Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Final Report*, London, 2019.
[118] Krasodomski-Jones, A., Smith, J., Jones, E., Judson, E., Miller, C., *Warring songs: Information operations in the digital age*, Demos, 2019, pp. 32-33.

the 2019 EP elections approached, European leaders acknowledged the importance of the threat. For instance, Commission President Jean-Claude Juncker stated in 2018 that 'in our online world, the risk of interference and manipulation has never been so high. It is time to bring our election rules up to speed with the digital age to protect European democracy'.[119] In 2019, with a clear view to the upcoming elections, Commissioner for Justice, Consumers and Gender Equality Věra Jourová stated: 'we cannot allow for election results in even one member state to be distorted by manipulation' and 'we are currently experiencing a digital arms race. Europe needs to be aware'.[120]

In this context, information operations have become especially salient in the European public debate. Indeed, many of the EU measures spearheaded by the Commission in preparation to the 2019 elections have focused on this facet of the threat. Most of these measures target one or more different types of disinformation (see Box 1). Other EU measures also targeted the funding and data management of European parties and foundations (cf. Chapter 5) and the risk of election-related cyber-attacks.

Box 1: Types of disinformation operations

Disinformation may be part of a foreign interference operation or come from domestic sources; at the same time, it may come from centralised actors, such as states or private operators, or from decentralised individuals and networks. If present, the operation's relationship with a given state may be of direct subordination or funding (state-directed), informal approval (state-sanctioned) or only consist in an alignment of goals without any role for state actors (state-aligned). Finally, disinformation actors may aim at causing harm and achieving political goals or simply at obtaining financial gains through ad revenues. It is important to note that domestic non-state sources may also be aligned to or backed by a foreign government.

Sources: Decker, B., *Adversarial Narratives: A New Model for Disinformation*, GDI, 2019, p. 11; EUvsDisinfo, *Methods of Foreign Electoral Interference*, 2019, https://euvsdisinfo.eu/methods-of-foreign-electoral-interference/.

The concerted European effort aimed at the protection of the 2019 elections becomes especially visible since the issuing of the Communication on tackling online disinformation: a European approach,[121] more than one year ahead of the elections. After that, the Commission issued the Code of Practice on Disinformation (CoP)[122] in September 2018, together with its Package of measures to secure free and fair European elections. The Package included a Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament;[123] an amendment proposal to the rules on European political party funding;[124] and guidance on the application of the GDPR.[125] The amendment to the Audiovisual Media Services Directive (AVMSD) in November 2018[126] then included important

[119] Juncker, J.C., *Free and fair European elections*, State of the Union, Brussels, 12 September 2018.
[120] DW, *EU elections: Commissioner warns of Russian meddling*, 13 May 2019.
[121] European Commission, *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Tackling online disinformation: a European Approach*, Cit..
[122] European Commission, *EU Code of Practice on Disinformation*, Cit..
[123] European Commission, *Commission Recommendation of 12.9.2018 on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament*, C(2018) 5949 final, Brussels, 12 September 2018.
[124] Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No. 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012.
[125] European Commission, *Guidance Document – Commission guidance on the application of Union data protection law in the electoral context*, COM(2018) 638 final, Brussels, 12 September 2018.
[126] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States

references to media literacy.[127] Finally, the Action Plan against Disinformation, launched in December 2018,[128] announced the institution of the RAS, the reinforcement of the East StratCom TF and the submission by the major signatories to the CoP (Facebook, Google and Twitter) of monthly reports on their implementation of the Code. Annex 3 provides a timeline of all main EU measures since then and until the May 2019 elections.[129]

The rest of this chapter will develop as follows. Section 3.2 presents the disinformation issues concerning digital platforms and social media and the instrument adopted to tackle them, the CoP. Section 3.3 explores the instruments and recommendations adopted to guarantee the coordination of the electoral authorities of MS and cyber-protection of their infrastructure. Section 3.4 focuses on the work of the East StratCom Task Force, while Section 3.5 analyses civil society, media literacy and innovation initiatives aimed at countering electoral interference and disinformation. Finally, Section 3.6 concludes.

3.2. The Code of Practice on Disinformation

3.2.1. The CoP commitments and their implementation

First announced in the Communication on tackling online disinformation[130] and developed by the Working Group of the Multistakeholder Forum on Disinformation Online – composed of major online platforms, their trade association and major advertisers –, the CoP was finally published in September 2018. The CoP resulted from the recognition that social media platforms and advertisers play a fundamental role in all major disinformation issues, and that any meaningful solution thus needs to address such a role. Social media may be manipulated through a variety of means:

- dissemination of false or misleading content with little traceability (disinformation circulation generally runs through various stages before being widely spread on social media, starting on anonymous websites and passing through closed networks and conspiracy communities);[131]
- personalised political messaging through the microtargeting of ads;[132]
- use of bots and inauthentic accounts to artificially increase the spread of content and simulate vast grass-roots support (a technique called astroturfing) in order to exploit eco chambers and favour polarisation;[133]
- use of bots and inauthentic accounts to disrupt social media campaigns through spamming;[134]
- gaming of algorithms in order to amplify content diffusion and favour the self-radicalisation of users towards more extremist, tendentious or false information.[135] This can happen both by taking

concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.

[127] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.

[128] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Action Plan against Disinformation*, Cit,

[129] See Chapter 2 for a summary of EU policies over the 2014-2020 period.

[130] European Commission, *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Tackling online disinformation: a European Approach*, Cit., pp. 7-9.

[131] Cesarini, P., 'Disinformation during the digital era: a European code of self-discipline', *Digital Issues*, No. 6, Annales des Mines, 2019, p. 3; See also Christie, E.H., *Political Subversion in the Age of Social Media*, Wilfried Martens Centre, 2018, pp. 9-10.

[132] Christie, E.H., *Political Subversion in the Age of Social Media*, Cit., pp. 3-5.

[133] Ibid, pp. 5-7.

[134] Krasodomski-Jones, A., Smith, J., Jones, E., Judson, E., Miller, C., *Warring songs: Information operations in the digital age*, Cit., p. 22.

[135] Rieder, B., Matamoros-Fernandez, A., Coromina, O., 'From ranking algorithms to "ranking cultures": Investigating the modulation of visibility in YouTube search results', *International Journal of Research into New Media Technologies*, Vol. 24, No.

advantage of sensationalism to attract views and clicks (e.g. through clickbait) and thus increase the content's relevance or by directly falsifying the content's relevance as perceived by algorithms (e.g. through so-called Google bombs).[136]

The use of a self-regulatory instrument was considered the first step to address an issue that constitutes a moving target, with constantly changing features and little information on best practices.[137] The CoP is made up of 15 commitments grouped into 5 pillars:

- Scrutiny of ad placements (aimed at taking ad revenues away from online purveyors of disinformation);
- Transparency of political and issue-based advertising (aimed at defining political and issue-based ads and implementing stronger transparency and identifiability rules for them);
- Integrity of services (aimed at identifying fake accounts, bots and networks of bot-driven inauthentic interactions);
- Empowering consumers (aimed at favouring users' awareness through identifiability of false content, prioritisation of authentic and authoritative information, exposure to multiple perspectives, media literacy and critical thinking projects and transparency of ad targeting);
- Empowering researchers (aimed at fostering partnerships with academia and civil society on the topic of disinformation and at granting researchers access to platform data).

The CoP was initially signed by Facebook, Google and Twitter, the trade association representing online platforms (EDIMA), Mozilla and trade associations representing the advertising industry and advertisers (EACA, IAB Europe, WFA and UBA). Microsoft also subscribed to the CoP, albeit 8 months later, on 22 May 2019; two national-level advertising industry associations have also joined, namely the *Association des Agences Conseils en Communication* (AACC) and *Stowarzyszenie Komunikacji Marketingowej* / Ad Artis Art Foundation (SAR).[138] While the original CoP required all signatories to submit a yearly report on its implementation, as part of the Action Plan against Disinformation Facebook, Google and Twitter agreed to submit monthly reports, starting with a baseline report in December until May.[139]

This section focuses on the implementation reports of the three major original signatory platforms plus Microsoft, and on their assessment; each of them owns one or more social media platforms and/or tools addressed by the CoP (Facebook and Instagram, YouTube, Google Search and Google News, Twitter, Bing and LinkedIn) and Google is also the global leader of the advertising industry, being estimated to account for more than half of all advertising revenues to disinformation sites.[140] A summary of their measures is provided in Table 3.1. Mozilla has mostly focused on funding and awareness-raising, and trade associations have similarly focused on promoting subscription to the CoP among their members.[141] While several independent researchers and think tanks, the European Regulators Groups for Audiovisual media services (ERGA) and the European Commission have all issued full or partial

1, 2018, p. 64; Bradshaw, S., 'Disinformation optimised: gaming search engine algorithms to amplify junk news', *Internet Policy Review*, Vol. 8, No. 4, 2019.

[136] Decker, B., *Adversarial Narratives: A New Model for Disinformation*, GDI, 2019, p. 9.

[137] Pamment, J., 'The EU Code of Practice on Disinformation: Briefing note for the new EU Commission', *Policy Perspectives Series*, Carnegie Endowment for International Peace: Partnership for countering influence operations, 2020, p. 11.

[138] European Commission, *Code of Practice on Disinformation: First annual reports – October 2019*, 2019, pp. 1-2.

[139] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Action Plan against Disinformation*, Cit., pp. 8-9.

[140] Fagan, C., Wright, L., *Research Brief: Ad Tech Fuels Disinformation Sites in Europe – The Numbers and Players*, GDI, 2020, pp. 4-5.

[141] Annual self-assessment reports, available at https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

reports on the CoP's implementation, the third-party report envisaged in the CoP and the EC's final assessment are expected in 2020.[142]

3.2.2. Assessment

Most analyses have praised the importance of the CoP and its results as a first step; in particular, the Commission has underlined the Code's importance as a framework for a more structured dialogue and as an opportunity for greater transparency in the platforms' policies.[143] However, several flaws in the Code itself and in its implementation hamper its effectiveness in tackling disinformation, and a reform of the system is needed.[144] When assessing the CoP's effectiveness (incidentally, most assessments focus on Facebook, Google and Twitter), issues may mostly be grouped into two broad sets: flaws related to the Code's ambiguity (resulting in the heterogeneity of measures adopted by platforms) and problems related to the absence of stricter oversight and commitments to transparency.[145]

Table 1: Summary of key measures implemented by each company

	Facebook	Twitter	Google	Microsoft
Pillar 1: Scrutiny of ads	Ban on false ads, monetisation ineligibility for inappropriate content. Repository of running ads.	Ban on false ads, monetisation ineligibility for inappropriate content. Repository of past seven days' ads.	Ban on misrepresentative ads, monetisation ineligibility for inappropriate content.	Ban on false ads, monetisation ineligibility for inappropriate content. Repository of past six months' LinkedIn ads.

[142] European Commission, *Daily News 05/05/2020*, 5 May 2020. https://ec.europa.eu/commission/presscorner/detail/en/mex_20_808.

[143] European Commission, *Code of Practice on Disinformation: First annual reports – October 2019*, Cit., pp. 1-2.

[144] Presidency of the Council of the EU, *Report of the Presidency to the European Council on 20-21 June, on countering disinformation and the lessons learnt from the European elections*, 10415/19, 21 June 2019, pp. 10-11.

[145] The assessment is based on an elaboration of several institutional reports, academic articles and grey literature on the CoP and its implementation. Besides the aforementioned preliminary assessment of the reports by the Commission, other relevant sources are: Bayer, J., 'Between Anarchy and Censorship. Public discourse and the duties of social media', *CEPS Papers in Liberty and Security in Europe*, No. 2019-03 CEPS, 2019, pp. 18 and 21-28; Berzina, K., Kovalcikova, N., Salvo, D., Soula, E., European *Policy Blueprint for Countering Authoritarian Interference in Democracies*, Cit., pp. 34-36 and 41-43; Butcher, P., *Disinformation and democracy: The home front in the information war*, 2019, pp. 9-11 and 18; Dittrich, P.J., *Tackling the spread of disinformation. Why a co-regulatory approach is the right way forward for the EU*, Jacques Delors Centre – BertelsmannStiftung, 2019; ERGA, *ERGA Report on disinformation: Assessment of the implementation of the Code of Practice*, Brussels, 2020; ERGA, *Report of the activities carried out to assist the European Commission in the intermediate monitoring of the Code of practice on disinformation*, Brussels, 2019; European Parliament, *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*, Cit., pp. 105-106; European Parliament, *Regulating Disinformation with Artificial Intelligence. The Effects of Disinformation Initiatives on Freedom of Expression and Media Pluralism*, Panel for the Future of Science and Technology, Brussels, March 2019; Leerssen, P., Ausloos, J., Zarouali, B., Helberger, N., de Vreese, C.H., 'Platform ad archives: promises and pitfalls', *Internet Policy Review*, Vol. 8, No. 4, Alexander von Humboldt Institute for Internet and Society, 2019; Lupion, B., *The EU Framework against disinformation: What worked, what changed and the way forward*, Democracy Reporting International, 2019; Monti, M., 'La disinformazione online, la crisi del rapporto pubblico-esperti e il rischio della privatizzazione della censura nelle azioni dell'Unione Europea (Code of practice on disinformation)', in Monti, M. (ed.), *La disinformazione online e il ruolo degli esperti nell'agorà digitale: una prospettiva transdisciplinare*, No. 11/2020, Federalismi.it, 2020, p. 282-305; Pamment, J., 'The EU Code of Practice on Disinformation: Briefing note for the new EU Commission', *Policy Perspectives Series*, Carnegie Endowment for International Peace: Partnership for countering influence operations, 2020; Polyakova, A., Fried, D., *Democratic Defense Against Disinformation 2.0*, Atlantic Council, 2019, p.12-15 and 22-23; Sounding Board of the Multistakeholder Forum on Disinformation Online, *The Sounding Board's unanimous opinion on the so-called Code of Practice*, 2018.

Pillar 2: Political & issue ads	Identifiability and in-ad sponsor disclosure of political[146] and issue ads[147]. Past seven years' political and issue ads included in the repository. Ad library report on political and issue ads. Verification process for political advertisers.	Identifiability of ads. EU political ads kept without limit in the repository. Verification process for EU political advertisers. *All political ads have been banned from the platform as of 22 November 2019.*	Identifiability and in-ad sponsor disclosure of political ads Repository of past seven years' EU political ads. Verification process for EU political advertisers.	Identifiability of ads, in-ad sponsor disclosure of ads on LinkedIn. Ban on political and some issue-based ads.
Pillar 3: Services' integrity	Takedowns of accounts, pages and groups engaging in malicious behaviour.	Takedown of accounts engaging in malicious behaviour. Library dedicated to content exposed as state-backed interference.	Block of accounts whose creation or login are abusive. YouTube's policy only bans impersonation, not coordinated malicious behaviour. Safeguards against artificial manipulation of engagement.	Detection and neutralisation of suspicious online activity and block of accounts engaging in automated behaviour. Prevention of manipulation of Bing's search results.
Pillar 4: Empowering users	Fact-checking partnerships to review content in 14 EU countries and the UK. Content and ads shared by politicians are exempted. Context information on publishers. Warning and fact-checking articles	Simple chronological order of Tweets available to users instead of personalisation of the feed. Ban on voting suppression content and vote-related misleading content.	Prioritisation of authoritative content in queries on news and civic issues. 'Fact Check Explorer' and mark-up tool to search and signal fact-checked content. YouTube features to promote	Partial available customisation of Microsoft Advertising ads. Review of sources on Microsoft News. NewsGuard browser plug-in on Microsoft Edge to provide reliability ratings on sources.

[146] All platforms have adopted somewhat different definitions of political advertising: Facebook https://en-gb.facebook.com/business/help/167836590566506?id=288762101909005; Twitter https://business.twitter.com/en/help/ads-policies/prohibited-content-policies/political-content.html; Google https://support.google.com/adspolicy/answer/6014595?hl=en; Microsoft https://about.ads.microsoft.com/en-us/resources/policies/disallowed-content-policies.

[147] Issue-based ads in the EU were ads that made reference to six issues deemed of importance within the Union: immigration, political values, civil and social rights, security and foreign policy, economy and environmental politics.

	alongside debunked content. 'Why am I seeing this ad/post' features. Prioritisation of authoritative content. Support to online safety and media literacy projects.[148]	Suggested redirection to authoritative sources only for vaccine- or self-harm-related content. Support to online safety and media literacy projects.	authoritative sources and content. Google News feature to provide plural perspectives. External support to fact-checking organisations. Support to online safety and media literacy projects.	Prioritisation of high-authority content on Bing. Bing features to provide plural perspectives and fact-checked information. Support to NewsGuard's digital media literacy program.
Pillar 5: Empowering research	Provision of detailed content data to selected projects. Ad repository. Support to deepfake research.	Foreign information operations repository. Content and ad data already available through the Twitter API.	Ad repository. Support to deepfake research.	Support to disinformation and deepfake research.

Source: Own elaboration from signatories' monthly and annual reports.

Ambiguity and heterogeneity: the ERGA defined the commitments as too general, leaving too much room to individual platforms to fail to implement or only partially implement some of them. For instance, the first pillar, committed to disrupting monetisation incentives and ad revenues for "relevant behaviour",[149] does not require disinformation-specific criteria for rejecting advertisers. This has also favoured a wide heterogeneity of measures depending on the platform: while some differences allow the commitments to be better adapted to each platform's specificity, the current situation hinders coordination and further action even at a terminological level, with different platforms adopting different concepts and terms to frame their measures (e.g. Google's focus on "misrepresentation" and Facebook's on "coordinated inauthentic behaviour"). Blatant cases of heterogeneity are the different relationships that platforms have built with fact-checkers and their different approaches to political and issue ads: each platform has adopted partly different definitions to identify the political ads for which further transparency was required, and only Facebook has developed a definition to identify issue-based ads. Single platforms also exhibit policy differences between countries, as in the case of Facebook's fact-checking partnerships, which only apply to some MS. Finally, some policies also differ arbitrarily according to the topic, with Facebook, Google and Twitter all focusing more efforts on vaccine disinformation than on other disinformation-prone topics such as climate change.

Transparency and oversight: the CoP does not provide indicators or benchmarks to assess the platforms' progress in the implementation of its commitments. As a result, platforms have heterogeneously provided data that is only partly appropriate for a thorough assessment. Takedown data (pillar 3), for instance, cannot be disaggregated; the data of information operations are not archived, except by Twitter; the ad data provided allows only for a limited number of different query types; and the information provided, in particular on each ad's targeted audience, is too general and

[148] The full list of sponsored projects for each platform is detailed in Annex 4. A relevant downside of many projects is that they have been directed to a selected audience of journalists and other relevant stakeholders, leaving aside broad sectors of society.

[149] European Commission, *EU Code of Practice on Disinformation*, Cit., commitment 1.

not comparable to the micro-targeting options available to advertisers. Researchers' access to data has been marred by limitations, bugs and delays. Furthermore, data and information are completely lacking on themes such as algorithmic operations (including prioritisation and demotion mechanisms) and users' complaints and utilisation of the tools available to them. As a result, it is difficult to actually assess the efficacy of specific measures in a comprehensive manner, while institutional and independent reports claim that many of them might actually be ineffective.

The absence of some relevant provisions and themes should also be mentioned:

- No due process guarantees on takedowns and de-prioritisation of content are required, hampering accountability;
- No guidelines are present on the treatment and training of human moderators.

A final issue is that some relevant players have not subscribed to the CoP. Moreover, its provisions have not been applied to all apps owned by the signatories. As a result, important platforms and/or communication tools such as Snapchat, TikTok, Whatsapp and Messenger are still not addressed by the CoP; however, according to VP Jourová, TikTok, is going to join the Code's signatories.[150]

The current debate on the reform of the CoP focuses especially on whether to maintain a loose self-regulatory instrument or move, instead, in the direction of a co-regulatory approach or, even, direct regulation. VP Jourová stated in early 2020: 'for me it is clear that … to achieve a healthy, balanced use of technology you will also need some degree of regulation, in particular addressed to the platforms'.[151] While direct regulation is generally considered too difficult to implement in a context where trust-building with platforms remains pivotal and information on best practices too scarce, a growing consensus seems to be building around the co-regulatory option; the latter is seen as a way of addressing the previous concerns while still increasing the role of the public sector, in order to avoid the use of a voluntary and loose instrument and address the risk of a possible privatisation of censorship. However, in the longer term, any regulatory option will also need to fit into a wider global strategy that tackles platform vulnerabilities on a scale matching that of their outreach, and not be limited to a single country or group of countries.

3.3. Transnational electoral coordination and cyber-defence

3.3.1. The European Cooperation Network on Elections

The European Cooperation Network on Elections (ECNE) was introduced by the 2018 Recommendation on election cooperation networks. The Recommendation called on all MS to set up national cooperation networks including all authorities with electoral competence or charged with monitoring and enforcing rules related to online election-relevant activities. A supranational forum of cooperation was established in the European Cooperation Network on Elections, which includes a point of contact for each national network as well as a Commission representative.[152]

The national networks were established in order to "facilitate the swift, secured exchange of information on issues capable of affecting the elections to the European Parliament including by jointly

[150] European Commission, 'Response to disinformation around COVID-19: Remarks by Vice-President Věra Jourová at the Read-out of the College meeting', *Press Corner*, Brussels, 10 June 2020.

[151] Jourová, V., *Opening speech of Vice-President Věra Jourová at the conference "Disinfo Horizon: Responding to Future Threats*, European Commission, Brussels, 30 January 2020.

[152] European Commission, *Commission Recommendation of 12.9.2018 on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament*, Cit., Recital 18-19 and art. 1-6.

identifying threats and gaps, sharing findings and expertise, and liaising on the application and enforcement of relevant rules in the online environment".[153] The EU-level Network was conceived as a forum for the exchange of information and practices among MS.

The ECNE held five meetings in 2019, of which three before the elections (21/01, 27/02 and 04/04), one immediately after (07/06) and one later in November (27/11). Besides its members, the Network's meetings also hosted representatives from the EP, the Presidency of the Council of the EU, the EEAS, the ERGA, the EDPS, the APPF, EUROPOL, the EDPB, and even the OSCE and civil society representatives. The topics on the agenda of the meetings were: exchange of information on disinformation campaigns and other relevant online activities, efforts to counter foreign interferences, the application of rules on offline electoral activities to online relevant contexts, assessments of cyber-threats, CoP implementation, media regulation and personal data protection, the implementation of the RAS and election networks at the national level and awareness-raising activities.[154]

3.3.2. Electoral cyber-defence

The Recommendation on election cooperation networks has also stressed the importance of MS preparing countermeasures and assessing risks in view of possible cyber-attacks to the European elections.[155] Cyber-attacks may target state electoral infrastructure directly or other stakeholders, in particular political parties and candidates. Tactics may include hacking-and-leaking of sensitive information, DDoS (Distributed Denial of Service), hacking of voter databases or manipulation of the election results.

The Commission has recommended that MS follow the Compendium on Cyber Security of Election Technology developed by the NIS Cooperation Group. The Compendium is structured as a sum of guidelines, among which MS may find the most suitable for their electoral infrastructure and voting systems. The Compendium's guidelines address crisis planning and response, development and auditing of infrastructure, technical measures to protect elections and specific security measures for different parts of the electoral cycle as well as auxiliary systems and stakeholders – political parties in particular.[156] Moreover, on 17 May the Council adopted a Decision and a Regulation establishing a common framework for sanctions and other measures targeting the authors of cyber-attacks against the Union or its Members.[157]

Cyber threats and national preparedness exercises have been discussed in the meetings of the European Cooperation Network on Elections. Moreover, on 5 April 2019 the EU MS, together with the EP, the Commission and the ENISA as observers, took part in a preparedness exercise at a European level. The exercise aimed to assess resilience levels of national and EU institutions and other stakeholders, enhance national, cross-border and supranational cooperation among different institutions, test crisis plans and procedures against cyber and hybrid threats and identify existing gaps

[153] Ibid.

[154] Minutes of the ECN's meetings, available at https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en#meetings.

[155] European Commission, *Commission Recommendation of 12.9.2018 on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament*, Cit., artt. 12-18

[156] NIS Cooperation Group, 'Compendium on Cyber Security of Election Technology', *GC Publication*, No. 03/2018, Brussels, 2018.

[157] Council Decision (CFSP) 2019/797 and Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

and further measures to be implemented.[158] A second exercise was held on 15 May, focusing instead on simulated attacks on a broader list of essential services before and after the elections.[159]

3.3.3. The Rapid Alert System

The RAS was announced in the Action Plan against Disinformation[160] and established on 18 March 2019. The System was conceived as a network of national contact points (embedded in the national election coordination networks) and a digital platform for sharing insights on disinformation campaigns and coordinating responses. All MS as well as EU institutions feed information to the System, with the network of national contacts coordinating their countries' contribution to the platform, and the EEAS's StratCom team, in conjunction with the EC, acting as a facilitator.[161] The RAS's mandate thus focuses on disinformation both in periods of electoral activity and in the absence of relevant elections and referenda. Its specificity is the possibility for institutions and national representatives to provide real-time alerts on detected disinformation campaigns, allowing for a swift and coordinated response. However, no alerts were signalled in the run-up to the European elections, and the platform's role has mainly been that of a repository of disinformation-related information provided by some MS.[162]

3.3.4. Assessment

The European Cooperation Network on Elections: the Network seems to have effectively fostered a higher degree of collaboration and information sharing among Member States, also prompting some of them to better coordinate all institutions (and in some cases also political actors) involved in the electoral process nationally.[163] The two-tier system, however, relies on the effective implementation of national cooperation networks by MS, which have exhibited differing degrees of actual cooperation and institutionalisation.[164]

Electoral cyber-defence: details of the preparedness exercises have not been disclosed, but no significant cyber-exploits were undertaken during the elections. While some MS (Ireland, the Netherlands, France, Finland and Germany) have abandoned or postponed their plans to digitalise their voting systems,[165] thus reducing their vulnerabilities, significant work involving in particular electoral stakeholders is needed to maintain adequate levels of electoral cyber-resilience in all MS. The preparedness of Emmanuel Macron's *En Marche!* during the 2017 French elections has widely been considered a best practice example.[166] Such an effort by the EU, however, remains particularly complex as electoral operations are an area firmly under the control of MS.

The Rapid Alert System: the RAS has been praised as an effective means of information sharing among MS and EU institutions;[167] however, the alert mechanism has never been triggered, and some accounts have also questioned the usefulness of the information actually uploaded to the platform, which was

---

[158] European Parliament, 'EU Member States test their cybersecurity preparedness for free and fair EU elections', *European Parliament – News*, 5 April 2019.

[159] ENISA, *Testing cooperation of EU CSIRTs Network during large-scale cyber-attacks*, 15 May 2019.

[160] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Action Plan against Disinformation*, Cit., pp. 7-8.

[161] European External Action Service, *Factsheet: Rapid Alert System*, 2019.

[162] Apuzzo, M., 'Europe Built a System to Fight Russian Meddling. It's Struggling', *New York Times*, 6 July 2019.

[163] European Commission, Minutes – Fourth Meeting of the European Cooperation Newtork on Elections, Brussels, 7 June 2019.

[164] Presidency of the Council of the EU, *Report of the Presidency to the European Council on 20-21 June, on countering disinformation and the lessons learnt from the European elections*, Cit., pp. 3-4; Lupion, B., *The EU Framework against disinformation: What worked, what changed and the way forward*, Cit., p. 10.

[165] ENISA, *Election cybersecurity: Challenges and opportunities*, 2019, p. 7.

[166] Vilmer, J.B.J., *Successfully Countering Russian Electoral Interference*, CSIS, 2018.

[167] Presidency of the Council of the EU, *Report of the Presidency to the European Council on 20-21 June, on countering disinformation and the lessons learnt from the European elections*, Cit., p.11.

allegedly unstructured and unstandardized. Moreover, only a handful of countries (France, the UK, Germany and the Baltic States) contributed significantly before the elections.[168]

The absence of alerts is likely to have stemmed from strict requirements for identifying foreign interference campaigns and the more granular nature of external disinformation operations during the elections. Also, the different degrees of participation are likely to have derived from different monitoring capabilities, but also from differing levels of awareness of the problem. A final issue is the limited transparency of the System, with journalists and researchers calling for access to data such as the number of incidents shared and each Member State's contribution.[169]

On paper, the RAS targets precisely one of the most threatening features of information operations, i.e. their quick and burst-like nature that leaves opponents with little time to react.[170] However, its use did not address this concern, and there is also no clear guideline on which reactions an alert would trigger. Chapter 4 further deals with the RAS's use in the context of the COVID-19 pandemic.

3.4. The East StratCom Task Force

3.4.1. The Task Force and its pre-election work

The EU East StratCom TF was reinforced with additional budgetary resources and personnel in view of the 2019 European elections, as announced in the Action Plan against Disinformation (see also Chapter 2).[171] As the 2019 elections approached, on 2 April 2019 the TF published a series of articles on Russian electoral interference on its site, focusing on its methods and past attempts.[172] Its Disinfo Review also published four issues specifically addressing the European elections and Russian attempts at meddling starting on 16 April, while several other issues made references to disinformation pieces targeting the EU and its relationship with its MS and citizens. It also held awareness-raising public meetings in several European countries.[173]

The TF exposed 998 disinformation cases attributed to Russian sources between 1 January and 26 May 2019, according to the EC.[174] More in detail, in the period between 1 April and 26 May it identified and debunked 455 disinformation pieces.[175] Of these, 149 made reference to the EU or to one of its MS; 73 were in Russian and 67 in one of the EU languages (see Table 3.2), while 9 were in other languages. The main sources of the contents reviewed by the TF were Sputnik (35 disinformation pieces) and RT (28) for those directly aimed at a European audience, while those in the Russian language came either from Sputnik (20) or from a multitude of other sources.

The Task Force has broadly identified five narratives in anti-EU disinformation:

- 'the elites vs the people', referring to uncaring, greedy or manipulative elites who deceive and disempower the population to keep power and wealth for themselves;

---

[168] Apuzzo, M., 'Europe Built a System to Fight Russian Meddling. It's Struggling', Cit.

[169] Lupion, B., *The EU Framework against disinformation: What worked, what changed and the way forward*, Cit., pp. 9-10.

[170] Krasodomski-Jones, A., Smith, J., Jones, E., Judson, E., Miller, C., *Warring songs: Information operations in the digital age*, Cit., pp. 30-34.

[171] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Action Plan against Disinformation*, Cit., pp. 5-6.

[172] EUvsDisinfo, *Russian Election Meddling and Pro-Kremlin Disinformation*, 2 February 2019.

[173] EUvsDisinfo, *European Elections: Are We Ready?*, 16 April 2019.

[174] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Report on the implementation of the Action plan against disinformation*, JOIN(2019) 12 final, Brussels, 14 June 2019, p. 3.

[175] EUvsDisinfo, *Disinfo Database*.

- 'threatened values', referring to the loss of authentic, Christian and family-based values in Europe, replaced among others by Islam, atheism and homosexuality;
- 'lost sovereignty' or 'threatened national identity', i.e. the manipulation of states and the loss of their independence to their larger European neighbours, to the Union itself, to NATO or to the US, and the threat to national identities posed by minorities and supranational elites;
- 'imminent collapse', hinting at a coming collapse of the Union due to various causes, such as immigration and the economic crisis;
- 'hahaganda', i.e. jokes and satire to divert attention from Russian actions or to smear individuals and institutions.[176]

Table 2: Expected audience of disinformation pieces between 1 April and 26 May 2019

	German	English	French	Polish	Italian	Romanian	Spanish	Finnish
Pieces	20	13	13	12	3	3	2	1

Source: Own elaboration from EUvsDisinfo, *Disinfo Database*

Other frequent narratives were the Russophobic attitude of Western countries and media, adopted to hide their own faults and at times pushed to the point of warmongering; and the denial of any election meddling by Russia. Furthermore, specific variants of the 'elites vs people' narrative focused on the powerless and corrupt nature of the EP and on the Nazi or barbaric roots of the EU. Narratives on the imminent collapse of the Union were instead scarce in the run-up to the elections. All the aforementioned narratives are rarely found in a 'pure' format, but rather intersect with each other, adapt to the changing context and opportunities and aim at delegitimising multiple targets, mixing the EU, the West, NATO and national governments, often building on already present cleavages and divisions. Moreover, they are intertwined with disinformation pieces referring to disparate topics and conspiracies – such as deep state operations – with the intent of sowing confusion.

3.4.2. Assessment

The East StratCom TF has generally been praised for its work since its inception, continuously prompting calls for it to be reinforced both in terms of funding and staff.[177] Despite being relatively underfunded – its EUR 6 million budget pales in comparison to Russia's estimated EUR 1 trillion spent on its propaganda outlets –,[178] it has proved able to effectively trace large amounts of foreign propaganda, also thanks to a broad network of contributors. However, as its role shifts from expert analysis to public debunking, the transparency and accountability of its work has been questioned: clear indications of what criteria are used to identify disinformation, and how it interacts with the entities named in its weekly review or with the contributors, are missing.[179]

Furthermore, the TF's role is beset by some inherent limitations to its effectiveness. A first limit is the effectiveness of debunking. Its work on the identification and reporting of Russian disinformation is

[176] EUvsDisinfo, *5 Common Pro-Kremlin Disinformation Narratives*, 2 February 2019.

[177] European Parliament, *Resolution: Foreign electoral interference and disinformation in national and European democratic processes*, P9_TA(2019)0031, Brussels, 10 October 2019.

[178] Gessant C. M. 'Borrell rejette les allégations de modification d'un rapport sur la désinformation', à la suite de pressions chinoises', *Agence Europe*, Brussels, 30 April 2020; European External Action Service, *Questions and Answers about the East StratCom Task Force*, 05 December 2018.

[179] European Parliament, *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*, Cit., pp. 97-98; Butcher, P., *Disinformation and democracy: The home front in the information war*, Cit., pp. 14-16.

particularly useful in order to better understand the features of the Kremlin's disinformation campaigns; debunking articles are however slow to react and much less likely to reach those who are most affected by that very disinformation.[180] Such a limit is only aggravated by the TF's limited means of communication and by the language barrier of its website, which was available only in Russian, English and German before the elections and has only recently been translated into Italian and French.

Secondly, the TF's mandate is restricted to disinformation coming directly from external sources. Acting under the EEAS's authority, the TF was born to adopt a "harder" and more "competitive" approach to external communication and propaganda, rather than to fact-check foreign or even domestic information.[181] Such a limit is thus inherent to the TF's original conception and well justified: broader actions would risk turning the TF into an institution directly intervening in the European internal debate and infringing on free speech. Indeed, it has already done so, prompting a motion from the Dutch Parliament requiring its fact-checking activity to be terminated after a notable contrast with Dutch media.[182] This rightly prevents the TF from addressing domestic disinformation, but also means that foreign disinformation spread by likely domestic proxies can only be addressed with difficulty.

3.5. Societal resilience, media literacy and innovation

3.5.1. Fact-Checking

The Commission announced in its April 2018 Communication that it would support the establishment of an independent European network of fact-checkers; the aim was to "establish common working methods, exchange best practices, achieve the broadest possible coverage across the EU, and participate in joint fact-checking and related activities".[183] This goal was attained through the creation of the SOMA (Social Observatory for Disinformation and Social Media Analysis) in November 2018.

SOMA is a project funded by the Horizon 2020 programme (EUR 1 000 000) and the Connecting Europe Facility (EUR 2 500 000).[184] It provides a European network of member fact-checkers with a platform that allows them to cooperate and take advantage of already-existing and in-development verification tools and additional data sources. Governmental organisations may also become members but are given a separate workspace so as not to interfere or influence the work of the independent fact-checkers. The EC is a funder, without any oversight role.[185]

The Observatory underwent a test period until June 2019 and currently counts 39 public independent and 4 government-related members. Among the former, many are research centres or companies, while fact-checkers are heterogeneously distributed across European countries: Greece, Italy, Finland, Luxembourg and Lithuania are the countries represented by fact-checkers.[186] SOMA members may take advantage of the platform's tools in their own work or also launch investigations with the support of other member organisations. During the test period its public products and activities consisted mostly

[180] European Parliament, *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*, Cit., p. 114; Lupion, B., *The EU Framework against disinformation: What worked, what changed and the way forward*, Cit., p. 9.

[181] Wagnsson C., Hellman, M., 'Normative Power Europe Caving in? EU under Pressure of Russian Information Warfare', Cit.

[182] Schenk, M., 'BREAKING: Dutch Parliament Approves Motion Calling To Disband EUvsDisinfo', *LeadStories*, 6 March 2018.

[183] European Commission, *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Tackling online disinformation: a European Approach*, Cit., pp. 9-10.

[184] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Report on the implementation of the Action plan against disinformation*, Cit., p. 7; Klossa, G., *Towards European Media Sovereignty*, European Commission, Brussels, 2019, p. 85.

[185] SOMA, *FAQ*, 2020.

[186] SOMA, *The Observatory*, 2020.

of conference participation and workshops; during the period between March 2019 and the European elections it also collected and made public a repository of 189 news articles related to the topics of disinformation, interference operations and social media platform measures.[187] This latter activity has now been scaled back, with only 7 further articles added after the elections; instead, the Observatory has begun to publish the first cooperative investigations on its site.

3.5.2. Media literacy

Faced with a threat exhibiting ever-changing features and strategies, both EU institutions and analysts have stressed the growing importance of media literacy as a way to enhance societal resilience to various types of information operations. Media literacy is defined, in Recital 59 of the amended Audiovisual Media Services Directive (AVMSD), as 'skills, knowledge and understanding that allow citizens to use media effectively and safely' in order to 'enable citizens to access information and to use, critically assess and create media content responsibly and safely'. Furthermore, it is stated that 'media literacy should not be limited to learning about tools and technologies, but should aim to equip citizens with the critical thinking skills required to exercise judgment, analyse complex realities and recognise the difference between opinion and fact'.[188] At the European level the media literacy approach has been twofold, focusing both on legislation and on awareness-raising initiatives.

As for the latter, in its April 2018 Communication the EC announced the organisation of a European Media Literacy Week, to be held yearly starting in March 2019. The Week was conceived as an opportunity to raise awareness and prompt policy makers, experts and teams leading media literacy initiatives to share ideas and best practices.[189] To this specific end, the EC organised a conference in Brussels on 19 March and created an EU-wide repository of projects and events at the local level, where organisers could share their own activities. In the period before the election the repository counted 345 different events and projects.[190]

The legislative approach is enshrined in the aforementioned amendments of the AVMSD. With the support of the Expert Group on Media Literacy, in November 2018 the EP and the Council approved a revised version of the Directive, placing further importance on the concept of media literacy. In article 33a, the Directive now requires MS to promote and take measures for the development of media literacy skills and to report on their implementation (by 19 December 2022). On the one hand, both media service providers and video-sharing platforms are included as relevant stakeholders who need to promote the development of media literacy skills in the EU; on the other, the focus is placed on 'all sections of society' and 'citizens of all ages',[191] which breaks with the traditional scope of media literacy projects (generally focusing on younger students).[192]

3.5.3. Innovation

The 'digital arms race' that interference operations represent requires a constant effort to understand the features of the threat and to research and develop effective instruments to counter it. In particular, some of the funds distributed by the Horizon 2020 European programme (in some cases under the FP

[187] SOMA, *Resources*, 2020.

[188] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.

[189] European Commission, *European Media Literacy Week 2019*, 2019.

[190] European Commission, *European media literacy events*, 2019.

[191] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.

[192] European Audiovisual Observatory, *Mapping of media literacy projects and actions in EU-28*, Strasbourg, 2016.

7 scheme) in the years before the 2019 European elections were specifically earmarked for projects related to disinformation, amounting to EUR 39 500 000 in total.[193] A detailed list of the projects is provided in Annex 5.

3.5.4. Assessment

Fact-Checking: Soma was still in its test period before the elections. While it requires its members to credit the platform for the work done with its tools,[194] a specific quantitative or qualitative assessment of its impact lies beyond the scope of this report. The reach of its fact-checking activities, however, seems limited to a few countries.

It is indeed positive that the EC has decided to support independent fact-checking organisations, as these groups remain separate from EU and national institutions and may also address domestic disinformation and internal-external chains of disinformation providers more freely and thoroughly. Moreover, this platform has remained operative even in the aftermath of the elections, differently from other networks, such as FactCheck EU. However, the SOMA case also highlights the importance of coordination with other existing initiatives (e.g. FactCheck EU and CrossCheck Europe) or, since June 2020, the EDMO.

Media literacy: The results of the revised AVMSD will not be reported until 2022, thus making any thorough assessment of the Directive's implementation impossible. However, it is commendable that the AVMSD has explicitly included video platforms among the media literacy stakeholders and has shifted the focus away from students only, as older cohorts are among the strata most susceptible to disinformation.[195]

While we do not have a broad mapping and assessment exercise of media literacy projects in recent years yet, we can rely on the 2016 mapping report compiled by the European Audiovisual Observatory[196] to identify potential pitfalls to be avoided. The report indicated that, the main aims of the mapped initiatives were the production of media literacy resources and the engagement of the end-user, focusing on critical thinking and media use skills. The scale of the projects was generally national and very rarely European, and the most targeted groups were 'teens and older students'.[197] As mentioned above, this latter aspect is indeed problematic, and a more balanced target should be preferred. Moreover, the national level of most projects meant that disparities between countries were present and significant.[198]

Innovation: The level of funding for disinformation-related projects is significant and signals the EC's commitment to the problem. As many projects are ongoing or have just ended, it is currently difficult to assess their impact comprehensively.

3.6. Conclusions

As the European elections were held between 23 and 26 May 2019, analysts and policy makers began to comprehensively assess what level of interference was present both before and during the elections and how successful those attempts were. Most studies seem to show that interference operations were present and sustained, but did not take the shape of a massive cross-national disinformation campaign

[193] Klossa, G., *Towards European Media Sovereignty*, Cit., p. 85.
[194] SOMA, *Observatory usage and editorial policy*, 2020.
[195] Guess, A., Nagler, J., Tucker, J., 'Less than you think: Prevalence and predictors of fake news dissemination on Facebook', *Science Advances*, Vol. 5, No. 1, 2019.
[196] European Audiovisual Observatory, *Mapping of media literacy projects and actions in EU-28*, Cit., pp. 27-30.
[197] Ibid, p. 29.
[198] Ibid.

or of coordinated cyberattacks.[199] It also seems that false, misleading and ideologically extreme content did not consistently influence the information flow on social media platforms.[200] The Commission thus stated that interference attempts were deterred by the EU measures.[201]

However, the encouraging results may be partly explained by a disinformation strategy less focused on totally or partly false information. Some reports have claimed that much disinformation content was not actually fabricated or misleading; it was instead accurate content from mainstream sources which was selectively spread to amplify opposing narratives, aimed at steady societal polarisation.[202] A significant portion of disinformation content may also be composed of non-factual statements focusing not on falsifying reality but simply on eliciting violent reactions by the audience.[203] As a result, an excessive focus on fact-checking as a solution might be actually misleading, faced with such a multi-faceted threat. Finally, even the East StratCom Task Force has warned about domestic actors learning from the Russian playbook,[204] to the point where it may be difficult to distinguish between truly domestic agents and foreign proxies. Therefore, while it seems fair to say that the EU was not targeted by a massive, cross-national interference campaign, it is harder to judge whether disinformation has indeed been limited or has changed strategies and aims, what its long-term effects will be and to what extent EU measures have indeed been a deterrent. Acting on the weak points of current measures thus remains paramount.

The EU institutional response to the challenge has been broad, varied and deserves praise. In particular, the CoP has been a first-of-a-kind attempt to tackle one of the most important facets of disinformation, i.e. the role of social media and advertising companies and the use of automated tools to influence the information flow on the platforms. The cooperation networks have fostered increased coordination at the national and European level. The East StratCom TF has provided useful data on the main source of false information and narratives, Russia, and the RAS has been set up to allow for an immediate response to typically quick disinformation "bursts". Finally, societal resilience and media literacy have been recognised as the only durable response to multiple disinformation tactics and have been supported through multiple means. This has happened in the face of significant institutional constraints: in particular, the EU cannot directly intervene in the election management of its members. Limits and shortcomings to the EU's action are present, however (see Table 3.3). Moreover, many of these measures and the threats they are meant to tackle do not stop between elections[205] – as Chapter 4 on COVID-19 disinformation clearly shows. Therefore, their further development and reform can all

---

[199] Szicherle, P., Lelonek, A., Mesežnikov, G., Syrovátka, J, Štěpànek, N., *Investigating Russia's role and the Kremlin's interference in the 2019 EP elections*, Friedrich Naumann Foundation, Political Capital, 2019; Sawiris, M, Dušková, L., Syrovátka, J., Győri, L., Wierzejski, A., *European elections in the V4*, GLOBSEC, National Endowment for Democracy, 2019; Sawiris, M, Dušková, L., Syrovátka, J., Győri, L., *European elections in Central Europe: Information operations and disinformation campaigns*, GLOBSEC, National Endowment for Democracy, 2019; Lupion, B., *The EU Framework against disinformation: What worked, what changed and the way forward*, Cit., pp. 16-17; Syrovátka, J., 'In Scrooge's boots: Lessons learned on disinformation from the 2019 European elections', *European view*, Vol. 18, No. 2, 2019

[200] Marchal, N., Kollanyi, B., Neudert, L.M., Howard, P.N., *Junk News During the EU Parliamentary Elections: Lessons from a Seven-Language Study of Twitter and Facebook*, Oxford Internet Institute, 2019.

[201] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Report on the implementation of the Action plan against disinformation*, Cit., p.1.

[202] Sawiris, M, Dušková, L., Syrovátka, J., Győri, L., Wierzejski, A., *European elections in the V4*, Cit.; Krasodomski-Jones, A., Smith, J., Jones, E., Judson, E., Miller, C., *Warring songs: Information operations in the digital age*, Cit., p. 23; Presidency of the Council of the EU, *Report of the Presidency to the European Council on 20-21 June, on countering disinformation and the lessons learnt from the European elections*, Cit., p. 4.

[203] Krasodomski-Jones, A., Smith, J., Jones, E., Judson, E., Miller, C., *Warring songs: Information operations in the digital age*, Cit., pp. 23-24.

[204] EUvsDisinfo, *EU elections update: Reaping what was sown*, 23 May 2019.

[205] Presidency of the Council of the EU, *Report of the Presidency to the European Council on 20-21 June, on countering disinformation and the lessons learnt from the European elections*, Cit., p. 9.

but be postponed (cf. Chapter 6).

Table 3: Protecting the 2019 EP elections: key measures and weak points

Fields	Measures	Weak points
Tackling disinformation revenues and diffusion on online platforms	CoP	Ambiguity and heterogeneity in the platforms' implementation. Little transparency and oversight. Absence of relevant themes: due process for removed or flagged content, algorithmic transparency, training of moderators.
Electoral coordination and cyber-defence	ECNE	Heterogeneous level of cooperation and formalisation among Member States.
	RAS	No use of alerts and limited usefulness of shared information.
	Cyber-defence	Need of coordination among Member States and with vulnerable stakeholders.
Detection and exposure of foreign disinformation	East StratCom Task Force	Lack of transparency and due process. No mandate to act on domestic sources, even if suspected of being proxies. Limited outreach to the public and to those most influenced by disinformation.
Societal resilience, media literacy and innovation	SOMA	Project still in its test phase during the elections. Limited geographical reach. Need of more coordination with other civil society projects.
	Media literacy initiatives	Traditionally too much focused on younger cohorts and with significant inter-country disparities
	AVMSD	Implementation reports will be available in 2022.
	Horizon 2020 projects	Several still in development during the elections.
Regulation of European parties (cf. Chapter 5)	Financing and data protection reform	Further monitoring needed. Still significant variation in the national regulations of political parties on foreign funding and donations.

Source : Own elaboration.

4. FOREIGN INTERFERENCES AND THE COVID-19 PANDEMIC

KEY FINDINGS

- Amidst the COVID-19 crisis disinformation has been rapidly spreading from Russia, China, and to a lesser extent Iran and Syria, and has constituted a problem of foreign interferences in the EU;
- Disinformation entails false health advices, conspiracy theories and narratives about the EU and US failures in the handling of the crisis. It is aimed at sowing confusion and misperceptions within the public and undermining the effectiveness and credibility of Western institutions;
- Russian disinformation comes from state-backed media outlets and European proxies and it is amplified through social media. Chinese disinformation echoes the Russian playbook, adding more overt diplomatic efforts and covert social media campaigns to deflect any criticism for the pandemic;
- The EU response is articulated. It has enhanced the activity of the East StratCom Task Force to track and expose disinformation, enforced the Code of Practice on Disinformation to push tech companies and platforms to enact self-regulation policies, and activated the Rapid Alert System;
- Foreign disinformation around the Covid-19 crisis raises concerns about the resilience of the EU and calls for integrated responses with NATO and the UN.

4.1 Introduction

'We're not just fighting an epidemic; we're fighting an infodemic', declared Tedros Adhanom Ghebreyesus, WHO Director-General at a gathering on foreign policy and security in Munich, in mid-February, referring to fake news that 'spread faster and more easily than this virus'. UN Secretary-General Antonio Guterres stated on 28 March that the 'common enemy is COVID-19, but our enemy is also an infodemic of misinformation'. On 5 April, the HR for Foreign Affairs and Security Policy Josep Borrell declared that 'misinformation and disinformation continue to proliferate around the world, creating an infodemic that accompanies this pandemic'.

According to international institutions officials, analysts, experts and professional fact-checkers, disinformation and misinformation vis-à-vis COVID-19 has spread rapidly and on a massive scale and constitutes a serious threat to public health, security and public action in the EU. The crisis has created fertile ground for disinformation, challenging the efforts of institutions to deliver effective communication.

In the context of the COVID-19 crisis, different disinformation strategies can be observed. Fully fledged disinformation was accompanied by subtler misinformation tactics according to the strategic interests of external actors. Fake news can also spread through individual media users, who unintentionally act

as channels of dissemination of false or misleading content that originated elsewhere.[206] The crisis revealed how blurred the line is between illegal informational content and legal content that can intentionally cause public harm, and between legitimate public diplomacy operations and manipulative foreign influence. This chapter provides an assessment of the wave of disinformation circulation in relation to the COVID-19 crisis, with a specific focus on foreign interferences and their implications for public action.

It will develop as follows. Section 4.2.1 discusses the media sources of COVID-19 related disinformation and singles out the foreign actors to which they are attributable. Section 4.2.2 focuses on the types and the contents of the narratives, while section 4.2.3 provides an explanation of the rationale behind their dissemination. The following section 4.3 is dedicated to the institutional responses. Specifically, section 4.3.1 discusses the responses of EU institutions, section 4.3.2 traces the response of social media platforms under the aegis of the European Commission and section 4.3.3 outlines the key actions in the fight against disinformation at the international level. Finally, section 4.4 concludes.

4.2 The pandemic, disinformation and hybrid warfare

4.2.1 Dynamics of disinformation: actors, sources and targets

According to some observers, disinformation and misinformation surrounding the coronavirus were already circulating in Europe by the end of January.[207] The first piece of coronavirus disinformation recorded appeared on the Russian state-funded Sputnik News on 22 January 2020. From the end of January onwards, the amount of disinformation increased considerably, while the infosphere was increasingly loaded with COVID-19 related information. Disinformation surrounding COVID-19 originated with several types of sources. However, in relation to foreign interferences, disinformation came from state-controlled media, government-aligned websites, coordinated social media and messaging app accounts. According to the EUvsDisinfo reports, updated monthly, disinformation about the COVID-19 crisis originated mainly in Russia, China, MENA countries, Iran and, to a lesser extent, the Western Balkans. Disinformation also spread from within Europe but, in this case, foreign media outlets based in European countries were responsible for it.[208]

Russia. From late January to the beginning of April, almost 150 cases of disinformation spread by Russia controlled media, especially Sputnik and RT, were reported by EUvsDisinfo.[209] These two outlets appear to be the most engaged in pro-Kremlin disinformation and misinformation campaigns, raising concerns for European security and the effectiveness of European public action, since they are generously financed and widely circulated among Western audiences. Initially, Russia controlled media started spreading conspiracy theories about the western and human origin of the virus. Moreover, these kind of conspiracy theories appeared to be part of a common trend led by Sputnik broadcasters in several countries under the Russian influence in the Eastern EU area, together with other

[206] For a systematic definition of disinformation, misinformation and contiguous concepts, see Chapter 1.
[207] EUvsDisinfo, 'Conspirational virus', *News and Analysis*, 30 January 2020.
[208] EUvsDisinfo, 'Disinformation on the Coronavirus – Short assessment of the information environment', *EEAS Special Reports*, 19 March 2020; EUvsDisinfo, 'Short assessment of narratives and disinformation around the Covid-19 pandemic', *EEAS Special Reports Update*, 01 April 2020; EUvsDisinfo, 'Short assessment on narratives and disinformation around the Covid-19/Coronavirus pandemic', *EEAS Special Reports Update*, 24 April 2020; EUvsDisinfo, 'Short assessment of narratives and disinformation around the Covid-19 pandemic', *EEAS Special Report Update*, 20 May 2020.
[209] This is the number of cases reported by the EEAS Special Report updated to 1st April 2020, with respect to Russian related disinformation. In the following period, this number has grown considerably. Moreover, with a thematic search on the Disinfo database almost 500 cases of coronavirus related disinformation can be documented.

government-aligned websites. Pro-Kremlin propaganda also came from state-controlled newspapers such as Rossiyskaya Gazeta and RIA Novosti, and radio stations such as Radio Vesti FM, which manipulated misleading information about Russian aid to Italy in order to discredit European institutions.[210]

China. Observers discovered ties between Chinese and pro-Kremlin disinformation, with China driven disinformation partly adopting the Russian playbook, on the one hand with the purpose of spreading false or unproven theories about the origin of the virus, and on the other hand emphasizing the display of gratitude by some European leaders for Chinese aid.[211] In addition, examples of Chinese propaganda have been documented in social media, where covert operations have seemingly been conducted. ProPublica has documented a network of Chinese maneuvered accounts involved in a coordinated influence campaign in the USA indirectly attributable to the Chinese government.[212] There is also evidence that Chinese disinformation came from bot accounts and state supported advertising on social media, aimed at depicting China as a global leader in the fight against the virus and discrediting the West.[213] Reports confirm a high level of coordination among different parts of the Chinese communication system and amplification of messages across different languages and communication channels. According to Freedom House, Chinese disinformation has run through covert and overt tactics: embedding state media content in mainstream foreign media; spreading disinformation through public diplomacy; purchasing online ads with state media content; amplifying propaganda with Twitter bots.[214]

MENA region and Iran. In the MENA region, the Syrian regime used the COVID-19 crisis to attack the EU and the USA, accused of perpetuating an economic war against Syria and diverting sanitarian aid from Syrian refugee camps.[215] Iranian authorities supported fake news that targeted the United States, backing Russian and Chinese disinformation efforts, along with covert information operations on social media that amplified the narratives of the Iranian government. These operations were led by the International Union of Virtual Media, a prolific Iranian internet group seeking to influence internet users by backing pro-government communications.[216]

To conclude, evidence of the dynamics of disinformation shows a complex picture: disinformation and misleading information came from state supported media, government-aligned websites and even traditional media, especially in the Russian case, and came along overt and covert state-backed strategies through social media and messaging platforms, as exemplified by the Chinese and Iranian cases.

[210] EUvsDisinfo, 'Coronavirus: the BBC challenges pro-kremlin reporting from Italy', *News and Analysis*, 01 April 2020.
[211] Beaumont P., Borger J., Boffey D., 'Malicious forces creating 'perfect storm' of coronavirus disinformation', *The Guardian*, 24 April 2020.
[212] ProPublica, *How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus*, 26 March 2020.
[213] Australian Strategic Policy Institute, *Covid-19 disinformation and social media manipulation trends*, 17 April 2020.
[214] Freedom House, *Beijing's Coronavirus Propaganda Has Both Foreign and Domestic Targets*, 20 April 2020.
[215] EUvsDisinfo, 'Short assessment of narratives and disinformation around the Covid-19 pandemic', Cit. p. 8.
[216] Woodruff Swan B., 'State report: Russian, Chinese and Iranian disinformation narratives echo one another', *Politico*, 21 April 2020; On the role of Iran, see Graphika's Report *Long-Running Iranian Influence Operation Returns to Social Media with Anti-US and Pro-China Messaging*, 15 April 2020 https://graphika.com/reports/irans-iuvm-turns-to-coronavirus/.

4.2.2 The main narratives of COVID-19 disinformation

Having outlined the main actors and channels of COVID-19 related disinformation, this section describes what types of narratives were spread and represented a foreign interference issue.

False health advice. Several fake and misleading cases of health information have been documented. The EUvsDisinfo database shows Kremlin-linked media News Front and South Front arguing that COVID-19 can be cured without vaccines and that China has blocked it with traditional medicine. Moreover, similar false claims were published in European audiences such as that 'COVID-19 can be cured with saline solution', that 'treatment for COVID-19 will lead to forced vaccination', that 'handwashing is useless for preventing the spread of the virus' (by Sputnik Germany), and that 'we have nothing to lose by making hydroxychloroquine publicly available without testing'. Other Kremlin linked media outlets in Europe spread conspiracy inspired news describing vaccines as means of mass control.[217]

This deliberately fake and fabricated information about the use of vaccines is matched by fake narratives claiming that the virus is spread to introduce mass control by the New World Order and to reduce the population. In this respect, South Front, one leading English language pro-Kremlin disinformation outlet, suggests that it is all fabricated by the Italian government to milk the EU for money and relax stringent EU budgetary rules.[218]

False health advice and misleading narratives about the health and medical management of the crisis was one major concern for international and public institutions. Moreover, disinformation related to conspiracy and false health advice going viral online has been increasing and is a cause for concern. Very often, as argued by EUvsDisinfo, most of this content is unintentional and those users who spread it are 'simply victims of deception' and indirectly contribute to the spread of narratives originating from external sources.[219]

Anti-institutional and conspiracy messages. In addition to false health narratives, disinformation takes the shape of political propaganda through the means of conspiracy theories and aims to discredit Western governments and EU institutions.

As an example, Russia backed media at first maintained that the virus originated in US military bases in China in order to weaponize it. Then these narratives were reposted by Chinese diplomats' spokespersons so as to deflect the blame for the Chinese origin of the pandemic. Other sources documented how behind the narrative of the Western origin of the virus lies the attempt of pro-Kremlin and pro-Beijing media to depict Russia and China as responsible partners in the fight against COVID-19. These narratives present Russia and China in a positive light and, at the same time, aim to overshadow EU and US actions to tackle the crisis.[220]

---

[217] Friends of Europe, *The dangers of the spreading 'disinformation virus'*, 28 April 2020.
[218] EUvsDisinfo, 'Short assessment on narratives and disinformation around the Covid-19/Coronavirus pandemic', Cit. p. 8.
[219] In this respect, it is worth noticing that pro-Kremlin media bandwagon on other conspiracy theories that have originated and spread via other channels. Cf. EUvsDisinfo, 'Capitalising on the Coronavirus conspiracist frenzy', *News and Analysis*, 14 May 2020.
[220] Barnes J., Rosenberg M., Wong E., 'As Virus Spreads, China and Russia See Openings for Disinformation', *The New York Times*, 28 March 2020.

As indicated by the EEAS Special Reports and confirmed by other reliable sources, there are several narratives targeting EU political and institutional efforts directly.[221] Pro-Kremlin sources, several domestic sources and proxies in EU Member States, the MENA region, the Western Balkans, and African countries have spread messages such as 'the EU is failing to deal with the pandemic' and 'the Union is about to collapse'. In the MENA region, for instance, the idea that the EU is 'dismantling' in the face of COVID-19 was widely propagated. In Ukraine, messages about the EU's imminent collapse were combined with the portrayal of Ukraine as a 'failed state' that was 'abandoned by its European allies'. Pro-Kremlin sources were particularly focused on Russian aid delivered to Italy, proclaiming that 'Russia is helping Italy and the EU is not': the state controlled Rossiya 1 TV channel maliciously reported that a Russian military convoy travelled on 'NATO roads'.[222] This event was investigated by the Italian newspaper *La Stampa* which discovered that the Russian reportage was recontextualised with misleading photos and narratives.[223] This is a clear example of Russian interference through a misinformation strategy, which builds on partially true facts and aims at generating and amplifying misperceptions among the public.

Such deliberately false or misleading narratives seek to represent Western institutions as less efficient at handling the crisis, thus affecting trust in public institutions. Finally, these narratives, especially those related to conspiracy theories, often look incoherent and chaotic, as they aim to sow confusion and disorient the public, making it more difficult for Western audiences to trust institutional communication and reliable information.[224]

4.2.3 Logics of disinformation: rationale and effects

Some preliminary evidence on the effects related to the influence of disinformation on European public opinion is already available. The Italian polling agency SWG conducted a survey finding that the share of respondents saying that they considered China to be friendly to Italy went up to 52% in March from 10% in January, while the share of respondents indicating they have trust in EU institutions went down to 27% in March from 42% in September.[225] According to an Ofcom survey reported by Al Jazeera, roughly 40% of adults in the UK were "finding it hard to know what is true or false about the virus".[226]

Professional fact-checkers agree that the widespread confusion partly stemmed from the overwhelming amount of available content online concerning COVID-19. Cristina Tardáguila, Associate Director of the International Fact-checking Network, has called COVID–19 'the biggest challenge fact-checkers have ever faced'. In this respect, an original survey conducted by the Reuters Institute for the Study of Journalism at the University of Oxford maintains that 'independent fact-checkers have moved

---

[221] Dempsey J., *Judy Asks: Is the Coronavirus Breeding Disinformation Across Europe?*, Judy Dempsey's Strategic Europe, Carnegie Endowment for International Peace, 09 April 2020.

[222] EUvsDisinfo, 'Short assessment of narratives and disinformation around the Covid-19 pandemic', Cit. p.9.

[223] On 25 March a reporter of the Italian newspaper *La Stampa* published an investigation about the Russian aids in Italy questioning their real usefulness and the strategic attempt of Russian authorities to instil divisions between Italy and its NATO partners. The article provoked the reaction of the Russian Ambassador in Italy, who maintained that Russia was not pursuing geopolitical interests through those aids. Moreover, Russia Defence Minister's spokesperson directly attacked the journalist, accusing him of 'nurturing Russophobia'. VP Věra Jourová tweeted in solidarity with the Italian journalist deeming the Russian declarations 'unacceptable'.

[224] Jakub Kalenský, *Six reasons the Kremlin spreads disinformation about the coronavirus*, Atlantic Council, 24 March 2020.

[225] See Bechis F., 'Infodemia, chi vince? I numeri di Swg e il dibattito al Centro Studi Americani', *Formiche.net*, 05 May 2020. https://formiche.net/2020/04/cina-usa-sondaggio-swg-casini-ventura/.

[226] Child D., Fighting fake news: The new front in the coronavirus battle, Aljazeera, 13 April 2020. https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2020/half-of-uk-adults-exposed-to-false-claims-about-coronavirus.

quickly to respond to the growing amount of misinformation around COVID-19; the number of English-language fact-checks rose more than 900% from January to March'.[227] Moreover, an analysis by the NGO Avaaz indicates that social media and especially Facebook are the epicentre of misinformation: the sampled content analysed was found to have been shared over 1.7 million times and viewed an estimated 117 million times. The analysis contends that 'millions of Facebook users are still being put at risk of consuming harmful misinformation on coronavirus at a large scale', and that Italian and Spanish-speaking users may be at greater risk of exposure, since Facebook has not yet issued warning labels on 68% of the Italian-language content and 70% of Spanish-language examined content, compared to 29% of English-language one.[228]

Given such evidence, a preliminary assessment of the logics of disinformation during the pandemic can be attempted. Disinformation is manifested as intentionally false or fabricated content either in the form of misleading or de-contextualised content. The major foreign actors backing this dissemination are prominently Russia and China, and their actions echo each other. More specifically, in the case of Chinese disinformation we can document overt tactics attributable to state officials, coupled by subtler covert tactics aimed at propagating pro-government propaganda through social media. In the Russian case, despite the Russian Health Minister publicly disconfirming conspiracy theories spread by Russian media, pro-Kremlin propaganda did not stop amplifying misinformation. The kind of interference at stake in the case of COVID-19 related disinformation is seemingly aimed at overloading the infosphere with contradictory messages in order to make it difficult for public authorities to be trusted, generating misperceptions and misunderstandings among the public that could undermine the effectiveness of European public action. Then, the strategy aimed at discrediting EU institutions runs in parallel with the attempt to present China and Russia as responsible and 'friendly' powers to European public opinion. According to the EEAS StratCom specialists, through a localised yet coordinated spread of disinformation, foreign interferences seek to undermine international cooperation and the multilateral system, with the West depicted as incapable of managing the crisis.

4.3 Institutional responses to disinformation on COVID-19

4.3.1 Institutional responses at the EU level

The European response to COVID-19 disinformation is elaborated in the framework of the European Action Plan on Disinformation and it should accordingly involve each European institution in a joint effort. The Plan serves to build the EU's capabilities and institutional tools to strengthen cooperation between MS on the issue of disinformation (Cf. Chapter 2).

With the COVID-19 outbreak European action against disinformation has become a primary concern at both the EU and national level. The European response to COVID-19 disinformation and foreign interferences has been formulated at several levels: a general improvement and efficacy of institutional communication; the enhancement of the EEAS's monitoring activities; the implementation of the CoP on Disinformation in order to push tech companies and platforms to adopt effective actions; the activation of the RAS to reinforce institutional cooperation between the EU and MS.

[227] Brennen J., Simon F. M., Howard P., and Nielsen K., *Types, Sources, and Claims of COVID-19 Misinformation, Reuters Institute*, University of Oxford, April 2020, p.1. https://reutersinstitute.politics.ox.ac.uk/types-sources-and-claims-covid-19-misinformation.

[228] Avaaz, *How Facebook can Flatten the Curve of the Coronavirus Infodemic*, 15 April 2020. https://secure.avaaz.org/campaign/en/facebook_coronavirus_misinformation/

The European Commission. On 31 March, the President of the European Commission Ursula von der Leyen launched a page on the Commission institutional website through a video, calling for public awareness on COVID-19 fake news and the perils disinformation could engender for the efficacy of the EU institutional response to the crisis. This appeal was addressed to European citizens in general, who were requested to only pay attention to trustworthy science authorities, national public health services and official information sources. For the Commission, the fight against disinformation is a joint effort involving all European institutions and a major concern to be addressed in the European Democracy Action Plan.[229]

The European Commission has worked in close cooperation with online platforms. VP Jourová encouraged tech firms and social media platforms to promote authoritative sources, discredit content that is fact-checked as false or misleading and take down illegal contents or content that could cause physical harm. Furthermore, the European Commission has promoted a series of counter-narratives in order to fight some of the main and most dangerous disinformation campaigns that are spreading through social media and mainstream foreign media as well as overshadowing authoritative communication.

The European Commission and the HR have framed the message that the 'EU's action will be fact-based and transparent, fighting any attempts of disinformation inside and outside the EU [and it] will also continue its engagement with global online platforms to facilitate access to authoritative health information'.[230] The European Commission communication has engaged in promoting responsible health information to mitigate the effects of conspiracy theories and false medical advices. It has extensively recommended that health advices should be taken from reliable and trusted sources, such as national public health authorities and the European Centre for Disease Prevention and Control, which works to communicate trustworthy and science-based advices jointly with the WHO.

On 10 June 2020, VP Věra Jourová and HR Josep Borrell have launched a joint communication calling for a much-calibrated response by the Commission and the EEAS to COVID-19 related disinformation and influence operations of third country actors.[231] The communication acknowledged that the crisis highlighted areas of fundamental challenges to be addressed with a systemic approach including MS, platforms, research networks and civil society, under the coordination of the EU institutions. The communication presented a roadmap to develop an effective response to disinformation. First, it stressed the importance of a correct understanding of the multifaceted nature of disinformation, which requires differentiated responses.[232] Second, the Commission and the EEAS should invest in enhancing strategic communication capabilities, in the EU public diplomacy and presence in national public debates. Third, the EU should enhance cooperation with MS through existing structures such as the RAS and with third countries and international partners.

Furthermore, social media platforms and tech companies should improve their transparency, enforcing and strengthening the policies that they have committed to implement under the CoP. In this respect,

---

[229] The European Commission response to disinformation is available at the dedicated webpage: https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/fighting-disinformation_en.

[230] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Communication on the Global EU Response to COVID-19.* JOIN(2020) 11 final, Brussels, 8 April 2020.

[231] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint communication to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions. Tackling COVID-19 disinformation - Getting the facts right*, JOIN(2020) 8 final. Brussels, 10 June 2020.

[232] As part of this approach, on 2 June 2020 the Commission launched the EU-funded European Digital Media Observatory, a multidisciplinary community composed of fact-checkers, academic researchers and other relevant stakeholders with expertise in the field of online disinformation. European Commission, Daily News 02/06/2020, https://ec.europa.eu/commission/presscorner/detail/en/mex_20_987

platforms will be required to report monthly on their policies in relevant areas, such as promoting authoritative contents, enhancing user's awareness, exposing and reporting manipulative behaviour referable to third actors and providing access to data for researchers and the fact-checking community. Moreover, the EU has called for other relevant digital stakeholders that are not yet signatories, such as WhatsApp and TikTok, to participate to the CoP.

Finally, the Commission and the EEAS will also work to guarantee freedom of expression and a pluralistic debate by supporting professional journalism and independent fact-checking both at the EU and MS level. Remarkably, as disinformation thrives where societies are more vulnerable, the EU aims at empowering citizens and raising public awareness about the threats of disinformation by several resilience-building measures, including digital education and media literacy.

The European External Action Service. In the fight against disinformation, the European Commission has worked in collaboration with the EEAS. The East StratCom TF's flagship project EUvsDisinfo has analysed disinformation trends, exposed disinformation cases and raised awareness about disinformation coming especially from Russian sources. Disinformation cases are debunked and collected in a rich database available to the public. EUvsDisinfo publishes short news and analysis articles, a weekly disinformation review, and produces a monthly special report on disinformation on COVID-19, with a particular focus on foreign interferences.

The European Parliament. The EP has backed the Commission on fighting disinformation, publishing a webpage and issuing official communication aimed at building public awareness on the damaging role of fake news. On 2 April, on the occasion of the International Factchecking Day, the EP confirmed its commitment to 'raising awareness of the dangers of disinformation, not only for citizens' health, but also for democracy'. On 17 April, the Resolution on the EU coordinated action to combat the COVID-19 pandemic and its consequences[233] recognised disinformation as a major health and social threat, urging the EU to establish a European information source in all its official languages to ensure and enhance citizens' access to verified information. It reiterated that free and independent media are crucial for ensuring that citizens are well informed during the crisis, thus improving the functioning of democracy. It also called on the European Commission and the Council to update the EU Global Strategy, to be quicker to react to external disinformation and to promote the EU's ambition of a geopolitical Union; in this respect, it recognised the major danger coming from Chinese and Russian influence, asking the Commission to enhance its strategic communication efforts.

The Rapid Alert System. The European Commission confirmed the activation of the RAS which was entirely dedicated to COVID-19 related alerts of disinformation.[234] The system was used by EU MS to share knowledge about disinformation 'coming from external sources', as stated by the VP Věra Jourová on 3 March. This tool is designed for sharing information and alerts on foreign or suspected disinformation and incentivizes a proactive effort to share knowledge about disinformation among member states and EU institutions. All EU MS have designated a national contact point for the monitoring of fake news and have also agreed on a specific threshold for the system to be activated. So far, the system has frequently been updated, receiving almost 300 messages from MS.[235]

National level responses. In this respect, it is worth mentioning the case of Italy, where the Presidency of the Council of Ministers instituted a TF for monitoring and fighting the spread of fake news related to COVID-19 on websites and social networks.[236] The aim of the TF is to promote strategic collaboration

[233] European Parliament, *Resolution on EU coordinated action to combat the COVID-19 pandemic and its consequences*, P9_TA (2020)0054, 17 April 2020.
[234] Stolton S., 'EU Rapid Alert System used amid coronavirus disinformation campaign', *Euractiv*, 10 March 2020
[235] The RAS works in collaboration with G7 members as it is also linked to the G7 Rapid Response Mechanism on disinformation.
[236] Presidency of the Council of Ministers (Italy), *Institution of the Monitoring unit for the contrast to the spread of fake news related to COVID-19 on the web and social networks*, 4 April 2020.

with fact-checking organizations, social media platforms and other public subjects, such as the Anti-Trust authority, in order to expose fake news, assess methods to make authoritative information more visible online, involve users and citizens in fake news identification and exposure as well as enhance societal awareness and resilience.

4.3.2 The Code of Practice and social media platforms

The European Commission has acted to implement the provisions of the CoP. Since 3 March VP Jourová has chaired regular meetings with major tech companies and social media platforms such as Facebook, Twitter, Microsoft, Google and others.[237] In their capacity as signatories of the self-regulatory framework of the CoP, these companies have been requested to advance their efforts to limit the online spread of fake news and harmful content. Jourová also declared that "if the voluntary measures taken by online platforms are found lacking this year, they could face further regulation".[238]

Facebook. Facebook has taken initiatives in two directions. On the one hand, it has built up a COVID-19 Information Centre which has directed almost 2 billion users to the resources made available by the WHO and other authoritative health institutions. The platform has furthermore worked closely with around 60 fact-checking organizations working in 50 languages all over the world. The company also announced the allocation of 1 million dollars to fund 13 fact-checking organizations in collaboration with the International Fact Checking Network.[239] Fact checking is aimed either at eventually removing contents deemed harmful for public health or reducing their distribution by showing warning labels. As an example, Facebook declared that it exposed almost 50 million disinformation contents with warning labels during the month of April and, in the Coordinated Inauthentic Behaviour Report, that it discredited numerous contents from pro-Kremlin News Front and South Front for "coordinated inauthentic behaviour on behalf of a foreign entity".[240] In addition, the platform wants to show messages in the News Feed to users who have interacted with harmful disinformation content that was removed and connect them to authoritative sources such as the WHO 'mythsbuster' webpage.

Twitter. On 18 March after weeks of criticism about the laxness of its content regulation policy, Twitter, initiated regulatory initiatives aimed at containing the spread of COVID-19 disinformation by removing content that fits into a broad definition of harmful as something that 'goes directly against guidance from authoritative sources of global and local public health information'.[241] This new policy includes removing content that denies health authorities' recommendations; provides a description of treatments that are not immediately harmful but are known to be ineffective; makes specific and unverified claims that incite people to action and cause widespread panic; contends that specific groups or nationalities are never susceptible, or are more susceptible, to COVID-19; makes false or misleading claims on how to differentiate between COVID-19 and another disease. The Twitter spokeswoman declared that Twitter was prioritizing the removal of content that could potentially cause harm, and that it was not taking action against every tweet containing incomplete or disputed information about COVID-19.[242] Twitter also said that it was granting researchers and software developers access to a real time dataset of tens of millions of contents published daily on COVID-19,

[237] European Commission, Daily News, 04 March 2020. https://ec.europa.eu/commission/presscorner/detail/en/mex_20_388.
[238] Pop V., 'EU, Tech Firms Renew Pact to Fight Coronavirus Disinformation', *The Wall Street Journal*, 11 March 2020.
[239] Kang-Xing Jin, 'Keeping People Safe and Informed About the Coronavirus', *Facebook newsroom*, 04 May 2020. https://about.fb.com/news/2020/05/coronavirus/.
[240] EUvsDisinfo, 'Short assessment of narratives and disinformation around the Covid-19 pandemic', Cit. p. 11.
[241] Hern A., 'Twitter to remove harmful fake news about coronavirus', *The Guardian*, 19 March 2020.
[242] Timberg C., 'On Twitter, almost 60 percent of false claims about coronavirus remain online-without a warning label', *The Washington Post*, 8 April 2020.

for the purposes of research and study. VP Jourová deemed Twitter's move 'a good step in the right direction'.[243]

WhatsApp. The WhatsApp messaging platform is considered fertile ground for the spread of harmful disinformation.[244] WhatsApp has implemented stricter policy measures on forwarding aimed at reducing the spread of messages that could be considered overwhelming by users. Under the new policy, if users receive a message that has been forwarded more than five times, they will only be able to send it to a single chat at a time.[245]

4.3.3 International responses

The issue of disinformation driven by foreign actors has concerned institutions at all levels of governance. International organizations have been gradually engaging in several initiatives to tackle foreign disinformation.

The United Nations. Notably, UN Secretary-General António Guterres has described the impact of coronavirus as 'the most challenging crisis we have faced since the Second World War' also warning about the 'global mis-infodemic'. The UN launched a new Communications Response initiative 'to flood the Internet with facts and science', while countering the growing volume of misinformation.[246]

The WHO, which is at the frontline of the crisis, has added a 'mythsbuster' section on its official websites where all unproven or overtly false health advice being spread online (e.g. drinking alcohol), fake narratives about the spread of the contagion (e.g. the link with 5G technology), and the potential scams concerning some miraculous cure or home-made preventions (e.g. eating garlic) are debunked.[247]

NATO. COVID-19 related disinformation has been addressed as a security threat as NATO itself was targeted by disinformation attacks. NATO Defence Ministers held a digital meeting on 15 April to discuss the response to the COVID-19 crisis. In this context NATO's Defence Ministers recognized COVID-19 related disinformation as a major international security challenge. In the subsequent press conference, Secretary General Stoltenberg underscored the importance of countering disinformation both from state and non-state actors and acknowledged that foreign interferences were trying 'to sow division in the Alliance and in Europe, and to undermine our democracies'.[248] To robustly respond to disinformation strategies, NATO has worked closely with the EU. As Secretary General Stoltenberg declared at a meeting between NATO and EU Defence Ministers, it is 'more important than ever to help our respective members and partners, strengthen the resilience of our populations and fight disinformation'. Moreover, while acknowledging the risks from Russian and Chinese campaigns against multilateralism, he expressed the belief that 'the best response to disinformation and propaganda is free and independent press, is the work of journalists'.

The EU and G7. Finally, further multilateral responses come from a Joint Statement by the EU HR and Canada's Minister of Foreign Affairs on 14 April. They stated that G7 partners and the EU were working to identify and respond to the spread of disinformation by activating the G7 Rapid Response Mechanism, linked to the EU's RAS. The G7 Rapid Response Mechanism on disinformation is a

---

[243] Culliford E., 'Twitter opens up data for researchers to study Covid-19 tweets', *Reuters*, 29 April 2020.
[244] Spring A, 'Coronavirus: Viral WhatsApp messages 'drop 70%', *BBC News*, 27 April 2020
[245] Hern A., 'WhatsApp to impose new limit on forwarding to fight fake news', *The Guardian*, 07 April 2020.
[246] United Nations, *Covid-19 Response: 5 ways the UN is fighting 'infodemic' of misinformation*, 2020.
[247] World Health Organization, *Coronavirus disease (COVID-19) advice for the public: Myth-busters*, https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public/myth-busters
[248] NATO, *Press conference*, 15 Apr. 2020. On May 14th, NATO published through its communication channels including YouTube, a video titled *How is NATO responding to disinformation on Covid-19?* https://shape.nato.int/news-archive/2020/video-how-is-nato-responding-to-disinformation-on-covid19

mechanism of response promoted by the Government of Canada since 2018, as part of its role as G7 president, to identify and respond to threats to democracies.

4.4 Conclusions

Since the WHO denounced the spread of a dangerous 'infodemic', there have been a variety of attempts by foreign actors to interfere in the EU's, and the US's, handling of the crisis. As we have seen, evidence from East StratCom TF, independent fact-checkers, researchers and analysts, highlight a sustained effort by Russia, China and, to a lesser extent, Iran and Syria, to engage in disinformation campaigns. Foreign interferences via disinformation during the COVID-19 crisis became a real concern for European security and institutional stability.[249]

The Kremlin's tactics were aimed at undermining confidence in Western governments by covertly sponsoring contradictory information and conspiracy theories and discrediting the European response to the crisis. They succeeded in sowing confusion among citizens and causing distrust of public institutions. Instead, the Chinese government focused more on reshaping its international reputation and deflecting the blame for the pandemic with an overt diplomatic effort to present China as a responsible power. Chinese state media also purchased political advertisements on foreign social media sites and covertly tried to amplify their propaganda efforts by using social media.

Since disinformation from abroad hit the EU suddenly, already at the end of January, the Union failed to provide an immediate response. Notwithstanding the initial hesitation, EU institutions subsequently developed a strategic communication campaign, with significant efforts made to combat health related disinformation, jointly with the WHO and ECDC, and in the related activity of debunking disinformation, which was carried out by the East StratCom TF.

The crisis challenged the efficacy of the tools envisaged by the Action Plan. In this respect, the European Commission put pressure on the CoP's signatories. Social media platforms have in turn implemented measures to label and discredit harmful content in collaboration with fact-checkers and the scientific community. However, these self-regulations pertain mostly to health-related contents deemed as harmful or that directly incite actions against public health recommendations.[250] The self-regulatory framework envisaged by the CoP may not be sufficient with respect to the actual scale of disinformation, and it may not be effective at combating specific propaganda contents attributable to external sources which aim to intentionally undermine trust in public institutions.

The RAS is currently dedicated to COVID-19 disinformation alerts. It constitutes a key instrument to develop an effective response to foreign interferences, as it enables both EU institutions and MS to comprehend the overall picture of disinformation threatening European democracies. However, the

[249] On 24 April 2020, *The New York Times* reported that the EUvsDisinfo's Special Report expected by 22 April had been released after having been corrected due to the pressure of Chinese officials. The case was soon reported by major press agencies worldwide. Some analysts warned that this kind of attitude towards the Chinese Communist Party could constitute a problematic precedent. On 30 April, the HR for Foreign Affairs and Security Policy had an exchange of views with members of the Foreign Affairs Committee in the EP, where he denied that the report was watered down. See Apuzzo M., 'Pressured by China, E.U. Softens Report on Covid-19 Disinformation', *The New York Times*, 24 April 2020; Gessant C., *L'UE rejette les allégations de pressions chinoises concernant un rapport sur la désinformation*, *Agence Europe*, 30 April 2020.

[250] The European Commission also welcomed a monitoring report by the European Regulators Group of Audiovisual Media Services on the effectiveness of the CoP. The report noted "significant weaknesses" of the CoP and called for more transparent, uniform, verifiable and binding measures to be taken by the platforms. Cf. ERGA, *ERGA Report on Disinformation, Assessment of the implementation of the Code of Practice*, 5 May 2020.

information collected through the platform is still unstandardized and its uploading is not coordinated at the national level.[251]

Finally, disinformation amidst the COVID-19 pandemic has proved to be an evolving threat to democracies and all the relevant players must be mobilised to counter it. As disinformation also concerns citizens' minds and sentiments, it could be unintentionally amplified by digital users. Greater efforts should be made to support civil society and citizen empowerment in order to combat disinformation from below (Cf. Chapter 3).

[251] Stolton S., 'Regulation against fake news 'very important,' Reynders says', *Euractiv*, 15 April 2020.

5. FOREIGN INTERFERENCES AND POLITICAL PARTIES

KEY FINDINGS

- National political parties are among the main targets of foreign interferences in Member States;
- As a response, most Member States have introduced bans on foreign donations to political parties and candidates, and comparative analyses show an overall trend towards further limitations, fostered by international pressures;
- However, potential loopholes remain as concerns, for instance: loans, donations from private companies with mixed ownership or from natural persons whose wealth originates abroad;
- The EU cannot regulate national parties, but it does discipline Europarties, which were the subject of two important reforms in 2018 and 2019;
- Regulation (EU, Euratom) 2018/673 determined that the budget of Europarties shall be covered by EU funds for a share of 90% (95% for foundations), thus reducing the amount of own revenues consisting of donations and membership fees;
- Regulation (EU, Euratom) 2019/493, on the other hand, introduced penalties for European political parties deliberately attempting to gain benefits from breaches of personal data protection rules;
- Overall, foreign influence on Europarties appears limited to a small share of donations (a mere 15% of which comes from outside the EU), which in turn only accounts for 10% of their total budget;
- Since European and national political parties are deeply interwoven, the issue of foreign interferences should best be tackled considering both levels.

5.1. Introduction

This chapter presents and reviews the main measures adopted to prevent foreign interferences in the activities of political parties both at the national and European level. As recalled by the EP in its Resolution of 10 October 2019, although 'the overwhelming majority of Member States have full or partial bans on foreign donations to political parties and candidates', in some cases 'foreign actors have found ways to circumvent them and have offered support to their allies by taking out loans with foreign banks'.[252] The Resolution explicitly refers to the loans and purchase agreements by the (then) *Front National* in 2016, the allegations that the *Freiheitliche Partei Österreichs* and *Lega per Salvini Premier* accepted dubious funding in 2019, as well as the opaque financial activities surrounding the Leave.EU campaign. The main country blamed for such interferences is Russia.

Since political parties are among the main targets of such attempted influences, adequate responses are needed. The EU regulates Europarties and their related foundations, but lacks the authority to discipline national political parties. Nonetheless, the financing of the latter also has clear implications

[252] European Parliament, Resolution of 10 October 2019 on foreign electoral interference and disinformation in national and European democratic processes (2019/2810(RSP)), recital 7.

for European political parties (EUPPs), which are ultimately composed of national member parties. Therefore, to understand and tackle the issue of foreign interferences in political parties, both the national and supranational level must be considered.

The rest of this chapter will develop as follows. Section 5.2 presents and briefly reviews some of the most recent cases of foreign interference in national elections since 2016. Section 5.3 first describes the measures adopted by MS to forbid or limit donations from foreign natural or legal persons (paragraph 5.3.1), then retraces an overall trend pushing for a stricter regulation of donations to political parties and candidates (paragraph 5.3.2). Section 5.4 adopts a supranational perspective, shifting the focus to European political parties. Paragraph 5.4.1 presents the rules concerning the financing of EUPPs as updated by the 2018 reform, while 5.4.2 examines the donations received, as well as their origin and distribution. The final paragraph (5.4.3) discusses the 2019 reform concerning the protection of personal data.

5.2. A review of the main foreign interferences since 2016

As discussed in the previous chapters (cf. Chapters 1, 4), foreign actors can influence public opinion or even the outcome of elections through a variety of means. This first section will describe some of the most recent cases of foreign interference in more detail. However, since the main focus will be political parties, special attention will be paid to formal and covert connections of national parties with foreign actors. Indeed, several European parties have been identified as having close ties with the Kremlin: the Austrian *Freiheitliche Partei Österreichs* (FPÖ), Hungary's *Fidesz* and *Jobbik*, Italy's *Lega*, France's *Rassemblement National*, Germany's *Alternative für Deutschland* (AfD) and the Brexit Party in the UK.[253] Those relations are sometimes driven by ideological affinity, and sometimes by material interests.

In **Italy** in particular, political parties have had long-standing relations with Russia, at least dating back to the *liaisons* of the Italian Communist Party with the Soviet Union.[254] More recently, Moscow has found new interlocutors in the emerging Eurosceptic parties, *in primis* the *Movimento 5 Stelle* and the *Lega* (formerly *Lega Nord*).[255] The latter party has even formalized the alliance by signing a deal with Putin's United Russia[256] concerning 'security, the defence of traditional values and future economic cooperation', in a similar guise to other documents signed with the (then) *Front National* (FN) of Marine Le Pen in France, or with the Austrian FPÖ.[257] Alongside these overt linkages, however, Matteo Salvini's *Lega* is suspected of more opaque forms of collaboration. For instance, the audio registration of a meeting held in Moscow in October 2018 publicly exposed an arrangement to funnel several EUR millions to the party, under a covert agreement to buy Russian oil.[258] Those political, economic and personal ties might allow Russia to exert some indirect influence on Italian politics across the political

[253] Klasa, A., Hopkins, V., Chazan, G., Foy, H. and Johnson, M., 'Russia's long arm reaches to the right in Europe', *Financial Times*, 23 May 2019; Klapsis, A., *An Unholy Alliance: The European Far Right and Putin's Russia*, Research Paper, Wilfried Martens Centre for European Studies, May 2015; Shekhovtsov, A., *Russia and the Western far right: Tango Noir*. New York, Routledge, 2018.

[254] De Maio, G., *Russia, Euroskeptic Parties, and Italian Elections*, Policy Brief, German Marshall Fund of the United States, 23 February 2018.

[255] Polyakova, A., Kounalakis, M., Klapsis, A., Germani, L.S., Iacoboni, J., de Borja Lasheras, F. and de Pedro, N., *The Kremlin's Trojan Horses 2.0: Russian Influence in Greece, Italy, and Spain*, Eurasia Center, Atlantic Council, November 2017, pp. 14-18.

[256] Seddon, M. and Politi, J., **'**Putin's party signs deal with Italy's far-right Lega Nord', *Financial Times*, 6 March 2017.

[257] Alandete, D. and Verdú, D., 'How Russian networks worked to boost the far right in Italy', *El País*, 1 March 2018.

[258] Nardelli, A., 'Revealed: The Explosive Secret Recording That Shows How Russia Tried To Funnel Millions To The "European Trump"', *BuzzFeed News*, 10 July 2019; Tizian, G. and Vergine, S., 'Quei 3 milioni russi per Matteo Salvini: ecco l'inchiesta che fa tremare la Lega', *L'Espresso*, 21 February 2019.

spectrum. Nonetheless, there have also been direct instances of alleged Russian interferences, primarily consisting of dissemination of fake news online, thus boosting anti-immigration narratives.[259]

Similarly, during the 2017 election campaign, **Germany** was hit by waves of disinformation spread on the Russian equivalent social media platform *Vkontakte*.[260] This and other Kremlin-backed broadcasters are suspected to have explicitly targeted the Russian diaspora, in support of the far-right party AfD: they allegedly translated fliers and tailored contents to the interests of that community.[261] Indeed, it is estimated that AfD enjoyed the support of one third of Russian-speaking residents in Germany, therefore it might not be surprising that 'among the party's core pledges on foreign policy is to lift German sanctions on Russia and seek warmer relations with President Vladimir Putin'.[262] Indeed, it emerged that some prominent personalities in the party (namely Frauke Petry[263] and Alexander Gauland,[264] both former AfD leaders) had met with members of the Russian parliament[265] in 2015 and 2017, although they strongly denied any collusion. Notwithstanding the media narratives spread online primarily benefitted the radical right, they have also had an impact on the broader political debate. One example is the huge resonance of the scandal involving Lisa, a German-Russian girl supposedly kidnapped and raped by Muslim refugees – a story soon belied by the police, but which ignited anti-immigration protests in the country.[266]

As already mentioned, the FPÖ in **Austria** is one of the European radical right parties with close ties to Russia. Heinz-Christian Strache, the head of the party, declared having met with US and Russian officials and having signed a partnership agreement with the latter in 2016.[267] The FPÖ was also at the core of a scandal following the release, in May 2019, of a video tape showing Strache and the leader of the party's parliamentary group Johann Gudenus attempting to obtain illicit financing from abroad in 2017.[268] The two were found discussing the possibility of secretly transferring funds to the party, in exchange for public contracts, with a young woman who they believed to be the niece of a Russian oligarch.[269] They were also reported suggesting that the woman buy half of the shares of the Austrian newspaper *Kronen Zeitung*, with the potential to gain huge influence on the tabloid's editorial line. Both Strache and Gudenus resigned following these revelations, leading to the fall of the coalition government with the *Österreichische Volkspartei*.[270]

Another party repeatedly meeting and collaborating with Putin — and bound by a cooperation deal with United Russia — is the *Rassemblement National* in **France**.[271] In 2014, Le Pen even borrowed around EUR 11 million from Russian banks, one of which (First Czech Russian Bank) was particularly close to the Kremlin perhaps in exchange for her support for Russian claims in Crimea.[272] Although firmly denying that such financing interfered with the National Front's positions, it was revealed that

[259] Interestingly, the Italian version of Sputnik is reported to be 'the second most-influential outlet in the Italian digital debate, only behind the US website The Huffington Post'. Alandete, D. and Verdú, D., 'How Russian networks worked to boost the far right in Italy', cit.
[260] Medium, '#ElectionWatch: Disinformation in Deutschland', 28 September 2017.
[261] Shuster, S., 'How Russian Voters Fueled the Rise of Germany's Far-Right', *TIME*, 25 September 2017.
[262] Ibidem.
[263] BBC News, 'German AfD leader Petry meets pro-Putin Russian MPs', 21 February 2017.
[264] Shuster, S., 'How Russian Voters Fueled the Rise of Germany's Far-Right', cit.
[265] Deutsche Welle, 'Head of the AfD Frauke Petry meets with Russian officials in Moscow', 20 February 2017.
[266] Meister, S., 'The "Lisa case": Germany as a target of Russian disinformation', *NATO Review*, 25 July 2016.
[267] Murphy, F. and Osborn, A., 'Austrian far right signs deal with Putin's party, touts Trump ties', *Reuters*, 19 December 2019.
[268] Bell, B., 'Austria scandal: Mystery of the honey-trap video', *BBC News*, 24 May 2019.
[269] Karnitschnig, M., 'Austrian government collapses over Russia scandal', *Politico*, 18 May 2019.
[270] BBC News, 'Austrian far-right FPÖ quits Kurz government after sacking', 21 May 2019.
[271] BBC News, 'France's Marine Le Pen urges end to Russia sanctions', 24 March 2017.
[272] Gatehouse, G., 'Marine Le Pen: Who's funding France's far right?', *BBC News*, 3 April 2017.

the party asked Russia for an additional EUR 27 million loan, with a view to financing the 2017 election campaign.[273] Besides financial matters, foreign interferences in the 2017 presidential elections seem to have primarily targeted Le Pen's opponent: Russian government-owned media outlets *Sputnik* or RT advanced allegations discrediting Emmanuel Macron[274] while hackers leaked his emails to release supposedly sensitive information.[275]

A variety of interference techniques were also deployed in the **UK**. In particular, the country was at the centre of the Cambridge Analytica affair, involving data harvesting from Facebook platforms to personalise politicised contents to the benefit of some political actors. An investigation was initiated in order to ascertain whether data owned by the Cambridge University Psychometrics Centre had been shared with people in Russia.[276] Social media also provided fertile ground for spreading anti-EU narratives during the Brexit referendum.[277] Whereas the impact of advertising appeared to be limited to a handful of cases,[278] fake accounts connected to Russia, although sometimes 'designed to look as if they were run from Ukraine', posted massively on the topic of the referendum, adding up to the disinformation spread by 'Kremlin-aligned media', such as RT and *Sputnik*, with 'a clear anti-EU bias'.[279] Moreover, the largest private donor for the Leave.EU campaign, Arron Banks, has had several meetings with staff from the Russian embassy, fuelling doubts that the money could be sourced from abroad.[280]

Foreign funding to political parties was not an issue in the **Netherlands** until 2017, when it emerged that Geert Wilders, the leader of the radical-right *Partij voor de Vrijheid* (PVV), had received conspicuous financial contributions from an American right-wing activist, David Horowitz.[281] Indeed, according to data released by the Dutch government, between 2015 and 2017 the total amount of PVV donations was EUR 155 833, of which EUR 137 133 came from American donors.[282] More recently, Thierry Baudet, leader of another conservative party, the *Forum voor Democratie* (FvD), was found to have had connections to Russia as some leaked texts messages hinted to payments he had received from the political analyst Vladimir Kornilov.[283] The latter was one of several undercover Russians who contributed to skewing the discussions on an EU trade agreement with Ukraine, during a Dutch (non-binding) referendum on the topic in 2016.[284] In fact, Kornilov spoke against the deal, presenting himself as a Ukrainian expat, when in fact he had been an advisor of the Russian government in the past.

Another campaign potentially affected by foreign interference was the referendum for the independence of Catalonia, in **Spain**. This was allegedly achieved primarily through online

[273] Oliveira, I., 'National Front seeks Russian cash for election fight', *Politico*, 19 February 2016.
[274] EUvsDisinfo, 'Emmanuel Macron in Russian Media', 16 February 2017; Schmidt, R., 'Russia, the far right, and anti-Macron bots', *EuObserver*, 3 May 2017.
[275] It is noteworthy that the attack was suspected to come from the same Russian-affiliated hackers that violated Hillary Clinton's mailbox during the 2016 US Presidential elections. Hern, A., 'Macron hackers linked to Russian-affiliated group behind US attack', *The Guardian*, 8 May 2017.
[276] House of Commons Digital, Culture, Media and Sport Committee *Disinformation and 'fake news': Final Report*, February 2019.
[277] EUvsDisinfo, 'UK, The Latest Target of Fake Russian Twitter Accounts', 17 November 2017.
[278] Cellan-Jones. R., 'Facebook and Twitter: Nine Russian Brexit ads found by inquiries, *BBC News*, 13 December 2017.
[279] House of Commons Digital, Culture, Media and Sport Committee *Disinformation and 'fake news': Final Report*, cit., p. 70.
[280] Cadwalladr, C., 'Arron Banks, Brexit and the Russia connection', *The Guardian*, 16 June 2018.
[281] Rubin, A.J., 'Geert Wilders, Reclusive Provocateur, Rises Before Dutch Vote', *The New York Times*, 27 February 2017.
[282] Mohdin, A., 'The Dutch far right's election donors are almost exclusively American', *Quartz*, 10 March 2017.
[283] Schaart, E., 'Dutch far-right leader Baudet had ties to Russia, report says', *Politico*, 17 April 2020; Rettman, A., 'WhatsApp leak exposes Russia link to Dutch far right', *EuObserver*, 17 April 2020. Forum voor Democratie denied the veracity of the content of these press articles.
[284] Higgins, A., 'Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote', *The New York Times*, 16 February 2017. Forum voor Democratie denied the veracity of the content of these press articles.

disinformation campaigns, whose location was traceable to the US,[285] Russia, and even Venezuela[286], which spread content hostile to the government. Examining the contents shared via social networks, it was found that hyperlinks referencing Russian media outlets exceeded in number those not only of some international, but even Spanish media.[287] This was also possible thanks to so-called 'bots': the majority of those contents (32%) came 'from *chavista* accounts or from Venezuela', 30% from anonymous accounts exclusively sharing RT or *Sputnik* contents, 25% from fake profiles, 10% directly from the two Russian media outlets and a mere 3% from real, individual profiles.[288]

Overall, in most recent cases of foreign interference in MS' election or referendum campaigns, the main culprit seems to be Russia. Other countries (e.g. the US or Venezuela) are only involved to a lesser extent. Influence was indeed exerted through different means: primarily by spreading false or misleading contents on social media thanks to automated accounts, but sometimes also supporting or funnelling funds to (usually right-wing Eurosceptic) political parties. Whereas the former issue might perhaps be more easily tackled through suitable countermeasures,[289] direct connections to political parties appear more difficult to regulate, since norms on party funding are often circumvented and the boundaries between the interest of the party and that of its individual members are blurred. Nonetheless, statutory provisions in that direction have been introduced, albeit in different forms and intensity, by most MS, which highlights the relevance of the topic in national agendas.

5.3. A legal map of party regulations in Member States

5.3.1. Bans on foreign funding: a comparative perspective

Connected to the risk of undue influence from foreign actors is the question of regulating the financing of political parties. Most MS have, in fact, introduced some restrictions to donations coming from abroad. This section will present and compare the measures adopted in different countries, building on the comparative political finance data which the International Institute for Democracy and Electoral Assistance (International IDEA) has been collecting since 2003. The information is gathered primarily on the basis of electoral or political party legislation, including decrees, regulations or subsidiary legislation. Researchers also consider legislation relating to political parties, the media, private companies or trade unions, as well as election reports or other political analyses conducted by experts or international bodies (e.g. the Group of States Against Corruption – GRECO).

For the purpose of the present work, the focus is on one of the four categories addressed by the International IDEA dataset, namely 'Bans and Limits on Private Income', referring to its latest version, updated in early June 2020. The tables in Annexes 6 and 7 provide information on the EU-28 in relation to bans on foreign donations to political parties and candidates. Table 5.1 (below) provides a summary of the findings, showing that 20 out of 28 countries (71%) have prohibited donations from foreign sources to political parties, and 18 out of 28 (64%) have forbidden foreign donations to individual candidates. Overall, it seems that the EU performs in line with — or even slightly better than — the

[285] Alandete, D., 'Pro-Russian networks see 2,000% increase in activity in favor of Catalan referendum', *El País*, 01 October 2017.
[286] Díez, A. and Mateo, J.J., 'Government confirms intervention of Russian hackers in Catalan crisis', *El País*, 10 November 2017.
[287] Alandete, D., 'How the Russian meddling machine won the online battle of the illegal referendum', *El País*, 13 November 2017.
[288] Alandete, D., 'Russian network used Venezuelan accounts to deepen Catalan crisis', *El País*, 11 November 2017.
[289] A detailed account of the measures introduced by some MS to combat foreign interferences, especially in the form of disinformation campaigns and cyber-attacks, is provided in a report by Carnegie. See Brattberg, E. and Maurer, T., *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, Carnegie Endowment for International Peace, May 2018.

OECD average: according to the OECD 2016 Public Governance Review,[290] 68% of member countries introduced bans on foreign donations to parties and 56% for candidates.

Table 4: Donations from foreign interests to political parties and candidates

1. Is there a ban on donations from foreign interests to political parties?			2. Is there a ban on donations from foreign interests to candidates?		
Value	Count	%	Value	Count	%
Yes	20	71	Yes	18	64
No	8	29	No	10	36

Source: International IDEA.

Recognising the potential uneasiness with such a dichotomous classification, the materials presented in the annexes add more nuances to the comparison by providing some additional information, illustrating some limits or exceptions to the bans. In fact, the countries that have put in place full bans on foreign donations are Austria, Cyprus, Estonia, Finland, France, Germany, Greece, Malta and Spain, joined by Italy in 2019. Conversely, Belgium, Denmark and the Netherlands are reported as having no restrictions on donations from foreign sources. Several other countries, however, present only partial restrictions.

To better grasp the potential interferences from foreign actors, the example of the US radical right movement lead by Donald Trump's former adviser Steve Bannon can be used. *The Guardian* attempted an analysis of countries that constituted easy targets for Bannon's project of coordinating populist radical right parties in the wake of the 2019 EP elections. Among them, Salvini's *Lega*[291] joined Bannon's 'The Movement', while other prominent leaders of populist right-wing parties in France and the Netherlands initially expressed their support.[292] Had that organisation intended to contribute financially to national party campaigns, however, it would only have been able to do so in Italy, Denmark, Sweden and the Netherlands. In countries with thresholds for foreign donations, such as Germany or Austria, its impact would, in fact, have been negligible; conversely, in Belgium despite the absence of formal bans against donations from abroad, all organisations are barred from making any contribution. Some influence could have been exerted, however, on Finland, allowing donations from like-minded individuals or groups.

Nevertheless, another difficulty lies in defining the very notion of 'foreign' in an increasingly globalised context, especially in the case of companies whose complex structures hinder the transparency of their ownership, which is often mixed.[293] Italy is a case in point, since companies are allowed to contribute financially to political activities if they pay taxes in Italy, but there is no provision to ascertain whether local offices are actually controlled by foreign interests. Contrariwise, this risk has been tackled in France since 1995 through the prohibition of donations from private companies, 'thus removing any

[290] OECD, *Financing Democracy: Funding of Political Parties and Election Campaigns and the Risk of Policy Capture*, OECD Public Governance Reviews, OECD Publishing, Paris, 2016.
[291] Horowitz, J., 'Steve Bannon's "Movement" Enlists Italy's Most Powerful Politician', *The New York Times*, 7 September 2018.
[292] Rankin, J. and Lewis, P., 'Bannon's Europe plan: a look at the law in his 13 targeted countries', *The Guardian*, 21 November 2018.
[293] Comai, G., 'Political funding and external interference: limits on donations, transparency, and controls', *Osservatorio Balcani e Caucaso Transeuropa*, 23 October 2019.

doubts regarding the nationality of the donor company and limiting spaces for donations by companies that under certain circumstances have a clear corruptive purpose (for example, donations in exchange for contracts or favourable laws)'.[294] Since 2018, in fact, only French citizens or people residing in France can make contributions to campaigns.

Similarly, in the case of natural persons it is equally possible that their source of wealth is foreign. This has been debated, for instance, in the UK, following allegations concerning the revenues of a British businessman who donated almost GBP 10 million to political forces supporting Brexit.[295] Therefore, an investigation by national authorities into the origins of money from large individual donors might also be particularly fruitful. Moreover, there might be other loopholes, for instance in provisions concerning loans relating to election campaigns: only 10 MS have introduced at least partial restrictions regarding loans taken out by political parties or candidates.[296]

These considerations highlight some of the undeniable limits of attempting a comparative classification of party regulations based exclusively on formal provisions relating to foreign finances.

5.3.2. Recent reform trends

The previous paragraph presented an overview of the provisions in force in MS. More recently, however, several countries have further reformed their legislation to tackle the issue of foreign donations more effectively. Overall, a trend towards a progressive restriction of provisions governing foreign donations to political parties or candidates in MS can be observed.

Perhaps the most radical restructuring of political financing was observed in **Italy**. Indeed, the country had been phasing out public party funding since 2014, and the 2018 elections were the first with exclusively private financing. Before the reform, as per decree-law No 149/2013, then updated by Law 13, 21 February 2014, there were no obligations to declare anonymous donations of up to EUR 5 000 received by parties or candidates and no limitations to funding coming from abroad. Overall, there was no apparent need for the introduction of measures preventing foreign funds from being used for domestic political activity. On the contrary, revenues from third countries seemed to be negligible: according to Transparency International, the only Italian parties declaring such funds were Silvio Berlusconi's *Forza Italia* and *Movimento 5 Stelle*.[297]

In early 2018, the transition to private funding was completed and the elections in March were held according to the new rules, thus allowing donations from foreign natural and legal persons. The incumbent government, however, soon introduced measures forbidding funding from third countries to parties, movements, foundations and related associations. It was part of an effort to curb corruption, strongly sponsored by the *Movimento 5 Stelle*, through law No 3/2019.[298] Only a few months later, nonetheless, Decree Law No 34/2019[299] allowed financing from abroad, albeit only if directed to foundations and associations, and provided that funds are not then redirected to political parties and

[294] Ibidem.

[295] Sloan, A. and Campbell, I., 'How did Arron Banks afford Brexit?', *openDemocracy*, 19 October 2017.

[296] In detail, restrictions concerning both parties and candidates have been introduced in France, Ireland, Malta and Slovenia. Restrictions to political parties only are in place in Bulgaria, Estonia, Latvia, Poland and Romania; restrictions referring exclusively to individual candidates are found in Cyprus. International IDEA: https://www.idea.int/data-tools/question-view/284560.

[297] Ferro, S. and Galinytė, A., *Partiti e fondazioni: quanto ne sappiamo davvero dei soldi ai politici?*, Transparency International Italia, Dossier No. 1, June 2018, p. 10.

[298] Legge 9 gennaio 2019, n. 3 - Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici. (18G00170) *(GU n.13 del 16-1-2019)*.

[299] Presidente della Repubblica, Decreto-Legge 30 aprile 2019, n. 34 - Misure urgenti di crescita economica e per la risoluzione di specifiche situazioni di crisi. (19G00043) *(GU n.100 del 30-4-2019)*.

movements. These new provisions, however, make it more difficult to detect irregularities in money transfers, since the plethora of organizations involved seriously hinders transparency.[300]

At present, however, it is forbidden for political parties and movements, as well as lists contesting elections in municipalities with a population above 15 000 people, to receive contributions from foreign governments and public entities and from legal persons based in a third country.[301] Similarly, natural persons not registered in the electoral register cannot make donations. On the other hand, it has been argued that this might limit other types of cross-border donations, such as funding for EP campaigns received by EUPPs.[302] Other important changes include a general ban on anonymous donations, a lowered threshold for disclosing the source of donations and reviewed sanctions for infringements of political financing rules.

In the **Netherlands**, in January 2018 the government announced its intention to ban foreign funding for political parties.[303] One year later, the prohibition on receiving money from outside the EU entered into force. This provision was combined with an increased effort towards proportionality, linking public funding to the number of seats held in parliament, notwithstanding the failure of the proposal to increase transparency by lowering the threshold for the publication of donations from EUR 4 500 to EUR 2 500.[304]

Another case of partial reform is **Romania**. According to the latest OSCE Report,[305] during Presidential electoral campaigns 'contributions from certain categories of donors, such as foreign sources, labour unions and state institutions and enterprises, are prohibited'. However, despite the introduction of some amendments to the Public Finance Law in July 2019, the provisions are not yet deemed stringent enough by OSCE, not only because 'detailed information related to the amount of each contribution and expenditure for each candidate is not required', but also because 'the law forbids the production and payment of campaign material by third parties' but still fails to address other potential forms of contribution or define third parties.

However, other countries have introduced the issue to the public agenda in recent times, and are soon expected to ban funding from third countries. **Denmark**, for instance, has been requested by GRECO reports to act in that direction since 2009.[306] A solid step forward came in May 2019, when the Danish parliament agreed that it would take action against actors who 'counteract and undermine democracy and fundamental freedom and human rights',[307] suggesting the creation of a list of foreign donors deemed anti-democratic to be banned from contributing financially to the activities of political parties and candidates. The text of the law was planned to be presented in the 2019/2020 session and become effective in 2021.[308]

---

[300] Transparency International Italia, *I finanziamenti esteri ai partiti sono leciti?*, available at: https://www.transparency.it/finanziamenti-esteri-ai-partiti-sono-leciti/.

[301] Camera dei Deputati, Servizio Studi XVIII Legislatura, *Disciplina e trasparenza dei partiti politici e delle fondazioni*, 22 April 2020.

[302] This was also noted in the case of Facebook's ban on cross-border advertising, harming some EU-centred investment for election campaign. Kayali, L. and de la Baume, M., 'EU on Facebook ad rules', *Politico*, 16 April 2019..

[303] Kroet, C.**,** 'Dutch ban on foreign funding for political parties would hit far-right PVV', *Politico*, 1 January 2018.

[304] 'PVV hardest hit as government bans non-EU political donations', *DutchNews*, 25 January 2019.

[305] OSCE, *Romania Presidential Election 10 and 24 November 2019 ODIHR Election Assessment Mission Final Report*, Warsaw, 26 March 2020.

[306] GRECO, *Third Evaluation Round - Evaluation Report on Denmark on Transparency of Party Funding (Theme II)*, 29 June-2 July 2009.

[307] 'Denmark agrees law against "antidemocratic" foreign donations', *The Local*, 3 May 2019.

[308] Ibidem.

Similarly, **Sweden** was put under pressure by GRECO in 2009, but decided to change its legislation accordingly in 2014. Although initially having no restriction whatsoever on donations financing political activities, in 2014 bans were introduced for foreign donations as well as anonymous donors (above a certain threshold).[309] It is also important to note, however, that the main source of funding for Swedish parties comes from public subsidies.

5.4. Regulating and financing Europarties

5.4.1. State of play after the 2018 reform

According to article 10(4) TEU, 'political parties at European level contribute to forming European political awareness and to expressing the will of citizens of the Union'. In the current denomination, also according to Regulation (EU, Euratom) No 1141/2014,[310] a European political party (EUPP) is defined as 'a political alliance which pursues political objectives and is registered with the Authority for European political parties and foundations' (art. 2(3)). More specifically, they are composed of national parties and/or individuals represented in several MS and organised in groups within the EP.[311]

In order to obtain registration from the already mentioned Authority, a party needs to be based in a MS, its member parties must not be affiliated to another European party and they must be represented in at least a quarter (seven) of the MS, considering the European, national or regional parliaments or, in alternative, have received, in seven or more MS, at least 3% of the votes at the most recent EP elections, as per Regulation (EU, Euratom) No 2018/673.[312] Moreover, the European party or its members must also have taken part in the EP elections or intend to do so in the next round, and must not pursue profit goals. Finally, European parties must observe the founding values of the EU, namely respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities (as expressed in article 2 TEU) in their programme and activities.

The Authority is in charge of registering, controlling and sanctioning European parties; it can even de-register them, via consultation of 'a Committee of independent eminent persons'.[313] In case funds are misspent, the Authority is also responsible for recovering the unduly paid amounts. According to Transparency International,[314] the most common irregular practices include pocketing the money for personal gain, hiring direct relatives as legitimately-funded parliamentary assistants (which was legal until 2014), or diverting funds to national parties or campaigns.

Several parties were banned after such irregularities in the use of funds were acknowledged. This was the case for instance of the Alliance for Direct Democracy in Europe (ADDE), related to the Europe for Freedom and Direct Democracy (EFDD) group, whose funding was suspended in 2016 after an audit disclosed the use of European funds in the 2015 British general election campaign.[315] Similarly, another

---

[309] Andreasson, L., 'Money in Politics - Why Sweden and Denmark Chose Different Paths. A Comparative Analysis of Party Finance Laws', 2019.

[310] Regulation (EU, Euratom) No 1141/2014 of the European Parliament and of the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations.

[311] For background information on the Europarties, see European Parliament, *Political Parties and Political Foundations at European level. Challenges and Opportunities*, Brussels, 2014 and Bressanelli, E., *Europarties after Enlargement. Organization, Ideology and Competition*. Basingstoke, Palgrave Macmillan, 2014.

[312] Regulation (EU, Euratom) 2018/673 of the European Parliament and of the Council of 3 May 2018 amending Regulation (EU, Euratom) No 1141/2014 on the statute and funding of European political parties and European political foundations, article 3(1).b and .ba.

[313] Ibid., art. 11.

[314] Aiossa, N., *3 ways MEPs can fiddle expenses*, Transparency International, 27 January 2017.

[315] Rankin, J., 'Defunct Eurosceptic party linked to Ukip asked to repay €1.1m', *The Guardian*, 30 May 2018.

report ascertained that the EUPP Movement for a Europe of Liberties and Democracy (MELD), and its related Foundation had used EU funding to promote the Danish *Dansk Folkeparti* during a general election and a EU referendum campaign[316] and to organise the activities of the party *Solidarna Polska* in Poland. Other allegations were raised against Marine Le Pen, suspected of having illicitly paid her party staff with money earmarked for parliamentary assistants or legislative tasks between 2011 and 2012.[317] In all these cases, parties or EP Members are expected to repay the appropriated amounts.

Since 2018, the funding has taken the form of contributions (previously it was an operating grant), whose rules are delineated in Title XI of the Financial Regulation.[318] Up to 90% of European parties' expenditures are covered by those contributions, while the remaining 10% should be covered by their own resources, usually membership fees and donations. This is quite a relevant change, considering that 85% of EUPPs' budget used to be composed of EU funds with a 15% share of own revenues. In order to be eligible for funding, European parties must be regularly registered, not subject to any sanctions by the Authority and audited by an external auditor mandated by the EP. It must also be represented by at least one MEP; the Commission in its proposal for Regulation (EU, Euratom) No 2017/0219[319] suggested increasing representation to three MEPs, but this provision was eventually dismissed.

If the abovementioned conditions are respected, EUPPs can apply for funding for each financial year, providing the EP with an estimated budget for the following year. 10% of the funds are distributed among worthy applicants in equal shares, whereas 90% is allocated in proportion to the number of elected MEPs belonging to each party (as per art. 19(1) of Regulation No 2018/673). This remains, however, a provisional amount, paid via pre-financing at the start of every financial year: the final contribution amount is determined after a revision by the EP Bureau of the annual reports submitted by the EUPPs. It must not exceed the provisional contribution nor the threshold of 90% of the costs actually incurred. This holds for both EUPPs and European Political Foundations (EUPFs).

However, Regulation (EU, Euratom) No 2018/673 has introduced other important changes. Until 2017, in fact, 15% of the total amount available was distributed equally to all parties meeting the requirement of having one MEP, leaving 85% to be distributed in proportion to each party's share of elected MEPs. The same distribution was also used for EUPFs. The present reform partially embraced the proposal of the Commission to reduce the equally distributed share to 5% to achieve 'a fairer and better reflection of electoral representation in Parliament'.[320]

Overall, the Commission noted a lack of clarity and transparency in the rules concerning the measures to be adopted if a party or foundation ceased to comply with the registration criteria, together with a general need to extend the scope of the measures to recover misspent funds. Other possible abuses pinpointed in the same Commission proposal concerned the numerical requirements — to be met either through representation in the EP, national or regional parliaments, or through support by individual members, or even both — and also the non-exclusivity of membership, since individual

[316] Jacobsen, H., 'European Parliament tells MEP to return €400,000', *Euractiv*, 6 May 2016

[317] Henley, J., 'EU watchdog asks Marine Le Pen to repay €339,000 in staff salaries', *The Guardian*, 31 October 2016.

[318] Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012.

[319] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No. 1141/2014 of the European Parliament and the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations.

[320] Ibid., p.5.

MEPs or national parties could sponsor more than one EUPP. The suggestions therefore included the possibility for national parties only to sponsor EUPPs, lowering the co-financing amount to 10% for EUPPs and 5% for EUPFs. As a matter of fact, EUPPs often encountered difficulties in reaching the 15% co-financing threshold, with relevant risks of circular financial flows or hardly quantifiable in-kind donations. Such changes were meant to increase transparency and publicity — as also recommended by the Court of Auditors.[321]

The justification of expenditures is conducted *ex post*, verifying whether the funding was used for licit reimbursable expenditures within the time limit, after which any unspent funding is to be recovered by the responsible authorising officer.[322] Using those contributions from the EU budget 'to directly or indirectly finance activities of third parties, in particular national political parties or political foundations at European or national level, whether in the form of grants, donations, loans or any other similar agreements'[323] is not allowed. In cases of infringement of such provisions, the contributions can be suspended, reduced or terminated.

Summing up, before 2018 85% of the budget of EUPPs and EUPFs was composed of EU funds, with 15% financed by own resources. Moreover, 85% of EU funds were allocated according to the seats held in the EP, the remaining 15% being distributed in equal shares to all EUPPs. Regulation (EU, Euratom) No 2018/673, instead, increased the share distributed proportionally to 90%, with 10% allocated in equal parts. More importantly, it has set the threshold of 90% as the share of EU funds for EUPPs (95% for EUPFs), decreasing the percentage of own resources to a mere 10% (5% for EUPFs). The latter provisions especially contribute to restricting the risks that foreign influence exerts on EUPPs through donations.

5.4.2. Mapping donations to Europarties

The amount of donations received by EUPPs and EUPFs has been steadily increasing: since the EP expanded its role as co-legislator with the Lisbon Treaty, stakeholders have an interest in supporting their preferred law-making initiatives through targeted financial contributions.[324] Before the 2014 reform, in line with most national restrictions, limitations applied to donations from anonymous contributors, from undertakings under direct or indirect influence of public authorities, and from any public authority from a third country. However, Regulation (EU, Euratom) No 1141/2014 has further restricted the requirements.[325]

For instance, all donations equal to or exceeding EUR 500 must be declared together with the name and legal address of the donor. However, payments under that sum are not classified as donations, therefore there is no legal requirement to provide details. Conversely, single donations cannot exceed EUR 12 000 (otherwise, they need to be immediately reported in writing to the Authority), and the total amount per donor per year must not exceed EUR 18 000 (art. 20). Parties cannot accept anonymous contributions, or donations from the budget of political groups in the EP (art. 222(6). Moreover, and most importantly here, they shall not accept:

[321] Court of Auditors Opinion No 5/2017 concerning the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 1141/2014 of the European Parliament and the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations.
[322] Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, cit., recital 163.
[323] Ibid., art. 222(3).
[324] Katsaitis, A., Assessing Interest Groups' Financial Donations to the European Union's Political Parties & Foundations, OECD Anti-corruption & Integrity Forum, 2018.
[325] Regulation (EU, Euratom) No 1141/2014 of the European Parliament and of the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations, cit.

> *(c) donations from any public authority from a Member State or a third country, or from any undertaking over which such a public authority may exercise, directly or indirectly, a dominant influence by virtue of its ownership of it, its financial participation therein, or the rules which govern it; or (d) donations from any private entities based in a third country or from individuals from a third country who are not entitled to vote in elections to the European Parliament.* [326]

The remainder of this paragraph will review the donations received by EUPPs between 2014 and 2017,[327] taking stock of data collected by the Authority and the EP on the basis of the individual EUPPs' declarations. An aggregated version of the data for the period of interest was retrieved from the website of the Dutch journalistic platform FTM.

Concerning the different types of donors (cf. Table 5.2 below), 56.9% is represented by ideologically close political parties or think tanks, although relevant shares are also covered by NGOs (17.9%) and private companies (16.9%). Furthermore, looking at the distribution of donations to the different EUPPs and EUPFs, distinguishing the origin of such contributions, a striking majority (77.3%) comes from EU MS, to which we can add other European transnational-based entities such as interest groups or think tanks (7.1%). The remaining 14.7% is, however, declared as coming from outside the EU and, within this group, the largest donor appears to be the United States. The only EUPP that declared it received funds from Russia is, interestingly, the EGP (from the Green Party of Russia).

Table 5.2 also shows that donations from the EU are primarily directed to the EPP (44%); other large recipients are the EGP (20%) and ACRE (13%). Donations from those that here are labelled as 'European transnational entities', are predominantly directed to the EGP (45%), followed by the EPP (34%); others do not exceed 10% of the total and several parties receive no donations at all from these sources. Finally, the largest recipient of funds from outside the EU appears to be the EPP (36%), followed by ACRE, ALDE and ADDE (16%, 15% and 13% respectively).

Overall, the risk of substantial foreign interference through the funding of political parties at European level appears negligible. In fact, considering that donations only contribute to up to 10% of EUPP financing, the fact that only 15% thereof originated from outside the EU is reassuring. On the other hand, establishing rules for national campaign financing vis-à-vis European elections remains the responsibility of individual MS.

Table 5: Types of donors, origin and recipients of donations to EUPPs and EUPFs, 2014-2017

Type of donors		
	Amount (EUR)	Share (%)
Political party / think tank	4 982 339.1	56.9
NGO	1 565 944.49	17.9
Private company	1 483 070.63	16.9
Individuals	446 061.6	5.1

[326] Ibid., art. 20(5). Emphasis added.

[327] Note that Regulation (EU, Euratom) No 1141/2014 only became applicable from the 2018 budget year (art. 40). The new rules further limit possibilities by foreign actors to influence EUPPs.

Unknown	209 306.15	2.4
Government / public sector	75 031.82	0.8
Journalistic platform	2 105.28	0.0
Total	*8 763 859.07*	*100*

Origin of donations		
	Amount (EUR)	Share (%)
From the EU	6 776 658.85	77.3
From outside the EU	1 284 534.02	14.7
From European transnational entities	622 018.08	7.1
Unknown	80 648.12	0.9
Total	*8 763 859.07*	*100*

	Recipients of donations					
	From the EU		*From transnational entities*		*From outside the EU*	
Party	Amount (EUR)	%	Amount (EUR)	%	Amount (EUR)	%
EPP (WMCES)	2 994 152.15	44%	210 715.03	34%	462 210.26	36%
EGP (GEF)	1 325 738.77	20%	282 306.44	45%	49 043	4%
ACRE (ND)	869 759.54	13%			204 765.27	16%
ALDE (ELF)	532 290.49	8%	58 911	9%	197 980	15%
EAF (EFF)	289 772	4%			69 385	5%
ECPM (SALLUX)	250 457	4%	46 974	8%	90 542	7%
EUD (OEIC)	154 579.73	2%			2 199	0%
ADDE (IDDE)	136 590	2%			164 829.49	13%
MENL (FENL)	102 500	2%				

EFA (CMC)	45 366.18	1%	23 111.61	4%		
EDP (IED)	43 090	1%				
EL (TE)	19 067.04	0%				
APF (Terra Nostra)	13 295.95	0%			7 580	1%
PES (FEPS)					36 000	3%
Total	*6 776 658.85*	*100%*	*622 018.08*	*100%*	*1 284 534.02*	*100%*

Source: own elaboration from Follow the Money. Note: EPP: European People's Party, WMCES: Wilfried Martens Centre for European Studies; EGP: European Green Party, GEF: Green European Foundation; ACRE: Alliance of Conservatives and Reformists in Europe, ND: New Direction - The Foundation for European Reform; ALDE: Alliance of Liberals and Democrats for Europe Party, ELF: European Liberal Forum; ECMP: European Christian Political Movement, SALLUX: Sallux; EAF: European Alliance for Freedom, EFF: European Foundation for Freedom; EUD: Europeans United for Democracy, OEIC: Organisation for European Interstate Cooperation; ADDE: Alliance for Direct Democracy in Europe, IDDE: Initiative for direct democracy in Europe; MENL: Mouvement pour une Europe des Nations et des Libertés, FENL: Fondation pour une Europe des Nations et des Libertés; EFA: European Free Alliance, CMC: Centre Maurits Coppieters; EDP: European Democratic Party, IED: Institute of European Democrats; EL: Party of the European Left, TE: Transform Europe; APF: Alliance for Peace and Freedom, Terra Nostra: Europa Terra Nostra; PES: Party of European Socialists, FEPS: Foundation for European Progressive Studies.

5.4.3. The 2019 reform of personal data protection

Regulation (EU, Euratom) No 1141/2014 and its subsequent reform required EUPPs, EUPFs, as well as MS and independent audit bodies controlling aspects related to the financing of EUPPs and EUPFs, to protect personal data against possible destruction, alteration or unauthorised access. They are also liable for any damage caused. The European Data Protection supervisor is responsible for monitoring and ensuring respect for and protection of fundamental rights and freedoms of natural persons, and it shall receive complaints from 'any data subject' (art. 33).

However, little was done to prevent and address the risk, exacerbated by online communication and media, of sensitive data being used to exert an improper influence on the political debate. One of the vastest manipulations of personal data was at the heart of the scandal involving Cambridge Analytica, a marketing and consultancy firm that (legally) harvested personal data from Facebook in order to generate tailored advertising.[328] Targeted advertising produced by abusing personal information probably affected the Brexit vote, since both Vote Leave and Leave.EU are suspected of having benefitted from the data breach. Moreover, according to the whistle-blower Christopher Wylie, data might have been shared with Russian companies tied to intelligence services.[329]

Similar events have triggered calls at the EU level for an increased protection of personal data: the Commission proposed an amendment to the Regulation in 2018,[330] as part of a 'security package' proposed at the Leaders' meeting in Salzburg (19-20 September). A debate within the LIBE Committee in the EP followed shortly after, underscoring the need to prevent the misuse of personal data.[331]

[328] Cadwalladr, C., 'The great British Brexit robbery: how our democracy was hijacked', *The Guardian*, 7 May 2017.
[329] 'Whistleblower: Cambridge Analytica Shared Data with Russia.' *Euractiv*, 17 May 2018.
[330] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 1141/2014 as regards a verification procedure related to infringements of rules on the protection of personal data in the context of elections to the European Parliament.
[331] LIBE Committee Press Release *Facebook-Cambridge Analytica: MEPs demand action to protect citizens' privacy*. 25 October 2018.

Regulation (EU, Euratom) No 2019/493 was approved in March 2019.[332] The new provisions target EUPPs, since the EU has no jurisdiction on national parties, but will also be complemented by recommendations issued to national governments in order impose stricter transparency requirements for political advertising online, thus curbing the practice of micro-targeting.[333]

In detail, sanctions can be imposed on EUPPs and EUPFs that deliberately attempt to influence the outcome of EP elections by exploiting infringements of personal data protection rules. A national supervisory authority will be in charge of acknowledging such breaches of the GDPR, which will then be referred to the committee of independent eminent persons already established under Regulation 1141/2014. The opinion of the committee will then inform the Authority's decision of whether to impose sanctions, consisting of a penalty amounting to 5% of the annual budget of the EUPP or EUPF involved and the suspension of EU funding for the following year.[334] Importantly, those fines are additional to the sanctions that national authorities can already impose for violations of the GDPR.[335]

This reform is important in the light of a comprehensive effort to prevent undue, broadly defined foreign interferences. In this sense, it is crucial that EUPPs ensure respect for privacy and the protection of personal data at all times during election campaigns.

5.5. Conclusions

Foreign influence has taken different forms, including the injection of funds into national political parties. The issue of party financing has been tackled in different ways. Despite the general trend towards more restrictive regulations of foreign donations, however, some problems persist when it comes to transparency and the weakness of control bodies. Moreover, some potential loopholes remain unaddressed in most MS, such as donations by companies or private individuals.

At the EU level, by reforming the regulations on party financing and cutting the percentage of own resources, the need for Europarties to secure external funding has been limited. Moreover, the data show that between 2014 and 2017 foreign donations only accounted for a small percentage of total donations, which are in turn a limited share of the revenues of EUPPs. Overall, the risk that foreign actors target EUPPs seems therefore considerably lower than for national parties. The guarantees provided by the latest reform concerning the protection of personal data, on top of the GDPR, seem to have further reinforced the security of the European space. In fact, the main risks of foreign interferences appear to materialise at the national level, upon which the EU can only exert pressure.

Coordination with MS to curb the risks of foreign interferences is therefore very important. Clear common guidelines or standards would be useful in this regard, also considering that funding for EP election campaigns primarily comes from national parties. At present, recommendations to MS come from other international organisations (e.g. Council of Europe's GRECO), but the introduction of EU standards would add to the international pressure for a stricter regulation of party financing from foreign donors.

---

[332] Regulation (EU, Euratom) 2019/493 of the European Parliament and of the Council of 25 March 2019 amending Regulation (EU, Euratom) No 1141/2014 as regards a verification procedure related to infringements of rules on the protection of personal data in the context of elections to the European Parliament.

[333] Khan, M., 'EU targets European political parties that misuse voters' data', *Financial Times*, 26 August 2018.

[334] Council of the European Union, Press Release, *EP elections: EU adopts new rules to prevent misuse of personal data by European political parties*, 19 March 2019.

[335] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1), art. 83(5).

6. POLICY RECOMMENDATIONS

This report has shown that foreign interferences are a major challenge for democracy. Election interferences, cyber-attacks, funding of political parties and disinformation campaigns endanger the functioning of democracy.[336] Malicious interferences ultimately weaken the trust of citizens in institutions and politicians and convey an image of democracies as regimes in decline, which are ineffective or incapable of responding to crises, particularly when compared to their authoritarian counterparts. Russia's 'hybrid warfare', in its different forms, has been a key security concern for the EU in the last few years. Its disinformation campaigns - well resourced, systematic and conducted on a larger scale than similar campaigns run by other countries – have necessitated strong reactions by the EU and democratic states more generally. On the other hand, Russia is not alone, and other states – first and foremost, China – are increasingly waging a 'war of narratives' with democracies.

Institutional and policy responses have been varied and multi-faceted. Both the EU and NATO have invested significant resources in strategic communication, setting up dedicated task forces to debunk, monitor and raise awareness of disinformation. Specific units have been set up to tackle hybrid threats (e.g. the European CoE for countering hybrid threats in Helsinki; the EU Hybrid Fusion Cell) and new mechanisms have been created to identify and quickly respond to disinformation 'bursts' (the Rapid Alert Mechanism). Specific actions have been implemented to minimise the risk of election interference, from the enhanced coordination of Member State authorities and electoral institutions through a dedicated network (the European Cooperation Network on Elections), to the attempt to (self-)regulate the content of social media platforms and improve their transparency (the Code of Practice on Disinformation). The funding of political parties, and their use of personal data, have also been further regulated.

Taking stock of all the policies, actions and tools developed in the last few years, the EU is now much better equipped to deal with hybrid threats and foreign interferences than it used to be in 2015. There has been strong leadership by both the European Council and the European Commission, and a constant push by the European Parliament – particularly through its resolutions – to step up efforts to counter the aggressive behaviour of Russia and other players. Clearly, this is a field in which the EU response complements national action. National governments remain in charge of protecting their elections and their media systems. Yet, given the transnational nature and the complexity of the challenge, uncoordinated individual responses are bound to be insufficient.

Building on the findings of the report, this concluding chapter makes specific policy recommendations to further strengthen the action of the EU and counter the threat of foreign interferences more effectively.

1) **Develop holistic and comprehensive approaches**. The EU should continue looking at foreign interferences in a broad way. Foreign interferences take several forms and cut across different policy domains. Effective responses require dialogue and coordination with national and local authorities and with international organisations (e.g. NATO). For instance, countering disinformation requires a broad set of measures like institutional responses (e.g. strategic communication units and information sharing), dialogue and engagement with social media platforms, projects with schools, the active involvement of civil society, financial support for independent journalism, fact-checkers and researchers. Although projects targeting society may

[336] Cf. also Council of the EU, *Council Conclusions on Democracy*, Brussels, 14 October 2019.

take time to bear fruit, a comprehensive approach appears to have, in the longer run, the most promising effects.

2) **Be quick**. Cyber-attacks and disinformation 'bursts' spread rapidly, but their consequences can be massive. This is even more so during electoral campaigns, when foreign interferences have the potential to produce instability and huge political costs for the affected actors. Institutional tools to counter them have to be efficient and capable of providing an immediate response. While the Rapid Alert System has been welcomed, the information collected through it is still unstandardized and not all MS seem to be equally committed to it. A desirable further development and reinforcement of this tool should aim at ensuring that MS *do* upload their information according to shared and more precise definitions and standards.

3) **Strengthen coordination structures.** To effectively counter foreign interference, MS should share their information and best practices, resisting the temptation to 'go it alone'; coordination should take place across countries, at the European and the international level. In this respect, cooperation in the context of the NATO CoE has been significantly enhanced and the EU itself has created new opportunities, such as the Cooperation Network on Elections, for dialogue and information sharing among MS. Such cooperation, particularly at the operational level, has to be further strengthened. By showcasing its positive effects (e.g. in the context of the 2019 EP elections) and providing guidance on best practices, the Commission could exercise pressure on the MS to step up their engagement and efforts.

4) **Communicate effectively with citizens**. Surveys have not only shown that citizens are worried about electoral interference and disinformation, but also that disinformation campaigns can produce significant changes in public opinion. The COVID-19 crisis has powerfully shown how countries like Russia and China seek to undermine the EU. In order not to succumb to their 'narrative warfare', the EU should not abandon the path already taken and should continue to invest in strategic communication. Further support for the StratCom Task Forces in terms of both financial and human resources is important. While the East StratCom TF has a growing staff of about 40 and a budget of 6 million euros, its resources pale if compared with Russian investments in the field. At the same time, the TF should improve the transparency of its working methodology and procedures.

   Furthermore, EU institutions themselves should become more visible to public opinion, engage with citizens and explain what they are doing. It is not sufficient to uncover 'fake news', a positive image of the EU has also to be more assertively framed and circulated. Having public opinion on your own side 'matters'. It is particularly important to make citizens aware of foreign interferences in the run-up to elections: on the one hand, this plays as 'deterrence' (i.e. it makes interferences less likely); on the other, it makes citizens wary of the issue and more sensitive to it.[337]

5) **Expand the reach of strategic communication**. The COVID-19 crisis has shown both that the amount of disinformation is cause for concern and that the sources of interference are expanding. Russia remains the key actor in the field, but China and, to a lesser extent, other states (e.g. Iran, North Korea) are also playing a more active role. While much effort is invested in monitoring

[337] Brattberg, E. and T. Maurer. *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*. Carnegie Endowment for International Peace. 23 May 2018.

Russian interferences – this is the specific mandate of the East StratCom TF – China is covered less. The EU should set-up a dedicated unit to debunk and monitor disinformation from China. Although the threat may appear less proximate compared to Russia, Chinese influence in the Western Balkans and in some MS (e.g. Italy) requires closer attention and firm responses. The recent call of the EP to update the EU Global Strategy and take a more proactive stance against both Russian *and* Chinese foreign influences seems to move in this direction.[338]

6) **Revise the Code of Practice**. The CoP had the great merit of establishing a structured dialogue with social media platforms and placing the issue of online disinformation high on the agenda. For some commentators, given the risks to freedom of speech inherent in any further attempt to regulate the field, 'the CoP arguably remains the best vehicle currently available'.[339] At the same time, however, the CoP has not fully met expectations. In the context of the COVID-19 crisis, as reported by Avaaz and other analysts,[340] Facebook's self-regulatory system still allows millions of users to see harmful misinformation contents before the platform labels or removes them. Twitter has been tardy in enacting such policies and a concerning amount of disinformation content still remains in the platform without any warning label. More generally, several concerns on the CoP have been raised regarding the ambiguity of its commitments and its lack of transparency and oversight.

   To overcome some of its main deficiencies, the CoP should become a co-regulatory instrument, maintaining trust and cooperation with platforms while ensuring greater oversight on them by EU institutions, by researchers and journalists. To this end, effective control instruments should be applied, and the benchmarks required for an effective assessment specified. The CoP should be extended to all relevant actors and commitments should be more precise, in order to avoid excessive heterogeneity of implementation. Due process guarantees, a workable definition of issue-based ads, increased transparency and accountability of algorithmic curation and better training of human moderators are aspects which should be considered in the revised version of the Code.

7) **Do not leave the 'left-behind' further behind**. Media literacy projects should be continuously sponsored and supported; building on the implementation reports of the AVMSD (by 2022), the EU should identify country disparities, best practices and target the most neglected sectors of society. Projects to support media reach and inclusion vis-à-vis fringe communities and individuals should be considered pivotal.

8) **Support journalists, fact-checkers and researchers**. Focus attention on supporting the growth and thriving of plural media ecosystems, based not only on established media outlets but also on medium-to-small independent outlets, which are much needed to enhance the resilience of healthy information ecosystems. In particular, projects such as SOMA should be replicated and better coordinated to target needy countries. Structures such as the newly constituted European Digital Media Observatory are important to encourage research cooperation across countries, gather new information on the 'anti-disinformation' policies adopted by online platforms and

[338] European Parliament, *Resolution on EU coordinated action to combat the COVID-19 pandemic and its consequences*, P9_TA (2020)0054, 17 April 2020.
[339] Pamment J. *The EU Code of Practice on Disinformation: Briefing Note for the New EU Commission*, Carnegie Endowment for International Peace, Policy Perspective Series #1.
[340] Avaaz, *How Facebook can Flatten the Curve of the Coronavirus Infodemic*, 15 April 2020.

provide independent policy advice. The overarching objective should be creating a more transparent and responsible debate in the digital sphere.

9) **Exert pressure on national parties to improve cyber-protection**. The Commission should set up a dialogue with political parties in MS to make them aware of cyber-security risks (e.g. on data protection) and ensure that they are well supported to step up their IT infrastructure to avoid data loss and the misuse of personal data. In March 2019, the Commission called on national parties to introduce rules on cyber-protection similar to the ones implemented with the 2019 amended regulation on European political parties.[341] Not only the Commission, but EU-level parties themselves should advise their national members on the required standards.

10) **Tighten the rules on foreign funding to political parties**. EU legislation could be amended to further reduce the share of co-financing for European political parties (bringing own resources down to 5% would align them with foundations). Furthermore, the Authority for European Political Parties and Foundations should be strengthened in terms of staff and resources, to enhance its scrutiny capacity and promote cooperation with MS for signalling cases of potential illicit funding.[342] The new European Public Prosecutor Office should also investigate alleged criminal offences related to the funding of European parties and foundations.

    Full transparency by national parties should be promoted concerning the revenues and expenditures for EP election campaigns. If ascertained that a national party contributed to an EP election campaign with foreign funds, their EUPP might be held responsible and eventually sanctioned. The Commission, but also Europarties themselves, should put pressure on (member) national parties to disclose the sources of their campaign funding and information on expenditure for online activities. It should not be forgotten that national parties affiliating with a Europarty are required to make this affiliation clear in their website, as a condition for a European political party's access to EU-funding. Lack of transparency should lead to fines and, for the most serious breaches, suspension of funding.

11) **Do not be complacent**. EU institutions should critically reflect on their weaknesses, which provide fertile ground for exploitation by third countries trying to interfere in the politics of the EU and its MS. A thorough understanding of the deficiencies of the Union provides a strong indication of the targets chosen by those organisations attempting to cause damage. Strategies to effectively confront hybrid threats and disinformation should not be a substitute or, worse, a 'cover-up', for the unwillingness or incapacity to bring about change.

[341] Jourová, V., *Note for the attention of the leaders of national political parties, foundations and campaign organisations in the context of the elections to the European Parliament*, Ref. Ares(2019) 1672467, 11 March 2019. https://ec.europa.eu/info/sites/info/files/letter_political_parties_final_en.pdf

[342] Cf. Kergueno, R., *Fraud and boats: funding European political parties*, Transparency International EU, 9 November 2017.

REFERENCES

EU official documents and websites

Council of the European Union, Press Release, *EP elections: EU adopts new rules to prevent misuse of personal data by European political parties*, 19 March 2019. https://www.consilium.europa.eu/en/press/press-releases/2019/03/19/ep-elections-eu-adopts-new-rules-to-prevent-misuse-of-personal-data-by-european-political-parties/

Council of the European Union. *Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats – Establishment and adoption of its Terms of Reference*. Brussels, 8 July 2019. https://data.consilium.europa.eu/doc/document/ST-10027-2019-INIT/en/pdf

Council of the European Union. *Council Conclusions on Democracy*. Brussels, 14 October 2019. https://data.consilium.europa.eu/doc/document/ST-12836-2019-INIT/en/pdf

Council of the European Union, *Complementary efforts to enhance resilience and counter hybrid threats - Council Conclusions*, 14972/19, Brussels, 10 December 2019. https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf

Court of Auditors, Opinion No 5/2017 concerning the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 1141/2014 of the European Parliament and the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations.

European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 1141/2014 as regards a verification procedure related to infringements of rules on the protection of personal data in the context of elections to the European Parliament. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1590423858080&uri=CELEX:52018PC0636.

European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No. 1141/2014 of the European Parliament and the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1590423917997&uri=CELEX:52017PC0481.

European Commission, High Representative of the Union for Foreign Affairs and Security Policy. *Joint Communication to the European Parliament and the Council. Joint Framework on Countering Hybrid Threats. A European Union response*. JOIN(2016) 18 final. Brussels, 6 April 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

European Commission, High Representative of the Union for Foreign Affairs and Security Policy. *Joint Staff Working Document. EU operational protocol for countering hybrid threats. 'EU playbook'*. SWD(2016) 227 final. Brussels, 5 July 2016. http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52016SC0227

European Commission, High Representative of the Union for Foreign Affairs and Security Policy. *Joint report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats – a European Union response*. JOIN(2017) 30 final. Brussels, 19 July 2017. https://ec.europa.eu/docsroom/documents/24601/attachments/1/translations/en/renditions/native

European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Report on the implementation of the Action plan against disinformation*,

JOIN(2019) 12 final, Brussels, 14 June 2019.
https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf.

European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Communication on the Global EU Response to COVID-19.* JOIN(2020) 11 final, Brussels, 8 April 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0011&from=EN

European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint communication to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions. Tackling COVID-19 disinformation - Getting the facts right*, JOIN(2020) 8 final. Brussels, 10 June 2020. https://ec.europa.eu/info/sites/info/files/communication-tackling-covid-19-disinformation-getting-facts-right_en.pdf

European Commission, *Commission Recommendation of 12.9.2018 on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament*, C(2018) 5949 final, Brussels, 12 September 2018. https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf.

European Commission. *Joint Communication to the European Parliament and the Council - A Strategic Approach to Resilience in the EU's external action.* JOIN(2017) 21 final. Brussels, 7 June 2017. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52017JC0021

European Commission. *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Tackling online disinformation: a European Approach*. COM(2018) 236 final. Brussels, 26 April 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236

European Commission. *Joint report to the European Parliament, the European Council and the Council on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018*. JOIN(2018) 14 final. Brussels, 13 June 2018.

https://eeas.europa.eu/sites/eeas/files/joint_report_on_the_implementation_of_the_joint_framework_on_countering_hybrid_threats_from_july_2017_to_june_2018.pdf

European Commission. *Joint communication to the European Parliament, the European Council and the Council - Increasing resilience and bolstering capabilities to address hybrid threats.* Join(2018) 16 final. Brussels, 13 June 2018. https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52018JC0016

European Commission, High Representative of the Union for Foreign Affairs and Security Policy. *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Action Plan against Disinformation*. 5 December 2018. https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf

European Commission, *Guidance Document – Commission guidance on the application of Union data protection law in the electoral context*, COM(2018) 638 final, Brussels, 12 September 2018. https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf

European Commission. *EU Code of Practice on Disinformation*. 26 September 2018.

https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

European Commission, *European media literacy events*, 2019. https://ec.europa.eu/futurium/en/european-media-literacy-events.

European Commission, *European Media Literacy Week 2019*, 2019. https://ec.europa.eu/digital-single-market/en/news/european-media-literacy-week-2019..

European Commission, *Code of Practice on Disinformation: First annual reports – October 2019*, 2019. https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019

European Commission, Minutes – Meetings of the European Cooperation Network on Elections, Brussels. https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en

European Commission. *2020 Work Programme: An ambitious roadmap for a Union that strives for more.* COM (2020) 37 Final. 29 January 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_124

European Commission. *Communication: Shaping Europe's Digital Future.* 19 February 2020. https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

European Commission. *Media Freedom Projects*, 2 March 2020. https://ec.europa.eu/digital-single-market/en/media-freedom-projects

European Commission, Daily News, 4 March 2020. https://ec.europa.eu/commission/presscorner/detail/en/mex_20_388.

European Commission. Daily News, 5 May 2020 https://ec.europa.eu/commission/presscorner/detail/en/mex_20_808

European Commission. Daily News, 2 June 2020

https://ec.europa.eu/commission/presscorner/detail/en/mex_20_987

European Commission, Official document: *Fighting Coronavirus Disinformation*, 29 April 2020. https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/fighting-disinformation_en.

European Commission, 'Response to disinformation around COVID-19: Remarks by Vice-President Věra Jourová at the Read-out of the College meeting', *Press Corner*, Brussels, 10 June 2020. https://ec.europa.eu/commission/presscorner/detail/en/speech_20_1033

European Council. *Conclusions.* Brussels, 20 March 2015. https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf

European Council. *Conclusions.* Brussels, 23 March 2018.

https://www.consilium.europa.eu/media/33457/22-euco-final-conclusions-en.pdf

European Council. *Conclusions.* Brussels, 14 December 2018.

https://www.consilium.europa.eu/media/37535/14-euco-final-conclusions-en.pdf

European Council. *Conclusions.* Brussels, 22 March 2019.

https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/en/pdf

European Council. *Conclusions.* Brussels, 20 June 2019.

https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf

European External Action Service. *Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy*. 28 June 2016. http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

European External Action Service. *Questions and Answers about the East StratCom Task Force.* 05 December 2018. https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en

European External Action Service, *Factsheet: Rapid Alert System*, 2019. https://eeas.europa.eu/headquarters/headquarters-homepage_en/59644/Factsheet:%20Rapid%20Alert%20System

European External Action Service. *Disinformation around the coronavirus pandemic: Opening statement by the HR/VP Josep Borrell at the European Parliament*. 30 April 2020. https://eeas.europa.eu/headquarters/headquarters-homepage/78329/disinformation-around-coronavirus-pandemic-opening-statement-hrvp-josep-borrell-european_en

European Parliament, *Political Parties and Political Foundations at European level. Challenges and Opportunities*, Policy Department for Citizens' Rights and Constitutional Affairs. PE 509.983. June 2014. https://op.europa.eu/en/publication-detail/-/publication/00c16095-d35a-4a17-9a5c-33decfee83c3/language-en/format-PDF/source-108311467

European Parliament. *Resolution on EU strategic communication to counteract EU propaganda by third parties*. P8_TA(2016)0441. 23 November 2016. https://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.html

European Parliament. *Resolution on Online platforms and the Digital Single Market*. P8_TA(2017)0272. 15 June 2017. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0272_EN.html

European Parliament. *Resolution on Foreign electoral interference and disinformation in national and European democratic processes*. P9_TA(2019)0031. 10 October 2019. https://www.europarl.europa.eu/doceo/document/TA-9-2019-0031_EN.html

European Parliament, *Foreign influence operations in the EU*, PE 625.123, Brussels, July 2018. https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2018)625123

European Parliament, *China's foreign influence operations in Western liberal democracies: An emerging debate*, At A Glance, PE 621.875, Brussels, May 2018.

https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2018)621875

European Parliament, *China's Maritime Silk Road initiative increasingly touches the EU*, Briefing, PE 614.767, Brussels, March 2018.

https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI%282018%29614767&utm_source=dlvr.it&utm_medium=facebook

European Parliament, *China, the 16+1 format and the EU*, PE 625.173, Brussels, September 2018.

https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2018)625173

European Parliament. *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States.* Policy Department for Citizens' Rights and Constitutional Affairs. PE 608.864. February 2019. https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2019)608864

European Parliament. *Recommendation to the Council and the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy concerning taking stock of the follow-up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda*

against it by third parties (2018/2115(INI). P8_TA(2019)0187. 13 March 2019. https://www.europarl.europa.eu/doceo/document/TA-8-2019-0187_EN.html

European Parliament. Interference from other countries in our democracies and elections. Topical debate. Strasbourg: 27 November 2019. https://www.europarl.europa.eu/doceo/document/PV-9-2019-11-27_EN.html#pvitem20

European Parliament, 'EU Member States test their cybersecurity preparedness for free and fair EU elections', *European Parliament – News*, 5 April 2019. https://www.europarl.europa.eu/news/en/press-room/20190404IPR35103/eu-member-states-test-cybersecurity-preparedness-for-free-and-fair-eu-elections.

European Parliament, *Regulating Disinformation with Artificial Intelligence. The Effects of Disinformation Initiatives on Freedom of Expression and Media Pluralism*, Panel for the Future of Science and Technology, Brussels, March 2019. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU(2019)624279_EN.pdf

European Parliamentary Research Service. The von der Leyen's Commission priorities for 2019-2024. PE646.148. January 2020. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646148/EPRS_BRI(2020)646148_EN.pdf

European Parliament (2020), Resolution: *EU coordinated action to combat the COVID-19 pandemic and its consequences*, P9_TA (2020)0054, 17 April 2020

European Union. *EU action plan on strategic communication*. Ares(2015)2608242. 22 June 2015.

Finland's Presidency Programme. *Sustainable Europe – Sustainable Future*. Presidency of the Council of the European Union 1 July – 31 December 2019. https://eu2019.fi/documents/11707387/14346258/EU2019FI-EU-puheenjohtajakauden-ohjelma-en.pdf/3556b7f1-16df-148c-6f59-2b2816611b36/EU2019FI-EU-puheenjohtajakauden-ohjelma-en.pdf

Flash Eurobarometer 464. *Fake News and Disinformation Online*. April 2018.

https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/82797

High-level Expert Group on fake news and online disinformation. *A multidimensional approach to disinformation.* Luxembourg: European Commission. March 2018. https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation

LIBE Committee, Press Release, *Facebook-Cambridge Analytica: MEPs demand action to protect citizens' privacy*. 25 October 2018. https://www.europarl.europa.eu/news/en/press-room/20181018IPR16525/facebook-cambridge-analytica-meps-demand-action-to-protect-citizens-privacy

High Representative of the Union for Foreign Affairs and Security Policy. *Joint Staff Working Document. Report on the Implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats.* SWD(2019) 200 final. 28 May 2019. https://data.consilium.europa.eu/doc/document/ST-9834-2019-INIT/en/pdf

Parliamentary questions. Answer given by Vice-President Mogherini on behalf of the Commission. Question reference: E-002156/2016. 23 June 2016. https://www.europarl.europa.eu/doceo/document/E-8-2016-002156-ASW_EN.html

Presidency of the Council of the EU, *Report of the Presidency to the European Council on 20-21 June, on countering disinformation and the lessons learnt from the European elections*, 10415/19, Brussels, 21 June 2019. https://data.consilium.europa.eu/doc/document/ST-10415-2019-INIT/en/pdf.

Joint Staff Working Document. *Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats*. SWD(2019)200 final. https://data.consilium.europa.eu/doc/document/ST-9834-2019-INIT/en/pdf

Jourová, V. *Opening Speech* of Vice-President Věra Jourová at the Conference "Disinfo Horizon: Responding to Future Threats". 29 January 2020. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_160

Juncker, J.C., *Free and fair European elections*, State of the Union, 12 September 2018. https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-free-fair-elections_en.pdf.

Special Eurobarometer 477. Wave EB 90.1. Report *Democracy and elections*. November 2018. https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/84538

von der Leyen, U. *A Union that Strives for More. My agenda for Europe*. Political Guidelines for the Next European Commission 2019-2024. https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

EU legislation

Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0796&from=EN

Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0797.

Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1808&from=EN.

Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0013&from=EN

Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1046&from=en.

Regulation (EU, Euratom) 2018/673 of the European Parliament and of the Council of 3 May 2018 amending Regulation (EU, Euratom) No 1141/2014 on the statute and funding of European political parties and European political foundations. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1590423970127&uri=CELEX:32018R0673.

Regulation (EU, Euratom) 2019/493 of the European Parliament and of the Council of 25 March 2019 amending Regulation (EU, Euratom) No 1141/2014 as regards a verification procedure related to infringements of rules on the protection of personal data in the context of elections to the European Parliament. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1590423989267&uri=CELEX:32019R0493.

Regulation (EU, Euratom) No 1141/2014 of the European Parliament and of the Council of 22 October 2014 on the statute and funding of European political parties and European political foundations. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1590424013003&uri=CELEX:32014R1141.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1590424137028&uri=CELEX:32016R0679

Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1046&from=en.

Other documents

AACC, *AACC Self-Assessment Report – Code of Practice on Disinformation*, 2019. https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019

AKA, *Code of Practise on Disinformation – Progress report*, 2019. https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

Camera dei Deputati e Senato della Repubblica, Legge 9 gennaio 2019, n. 3 - Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici. (18G00170) *(GU n.13 del 16-1-2019)*. https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2019;3

Camera dei Deputati, Servizio Studi XVIII Legislatura, *Disciplina e trasparenza dei partiti politici e delle fondazioni*, 22 April 2020. https://www.camera.it/temiap/documentazione/temi/pdf/1104961.pdf

CISA, *Election Security*. https://www.cisa.gov/covid-19-and-elections

Council of Europe, *Information disorder: Toward an interdisciplinary framework*, Council of Europe Report DGI(2017)09, Strasbourg, 17 September 2017.

Council of Europe, *LIBE exchange of views on disinformation in COVID-19 time*, Press release, Strasbourg, 12 May 2020. https://www.coe.int/en/web/freedom-expression/-/libe-exchange-of-views-on-disinformation-in-covid-19-time

Council of Europe. *Improving the protection of whistle-blowers all over Europe.* Reply to recommendation. Doc. 15099. 29 April 2020. http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=28634&lang=en

Council of Ministers Presidency (Italy), Decree: *Institution of the Monitoring unit for the contrast to the spread of fake news related to COVID-19 on the web and social networks*, 4 April 2020.

EACA, *EACA Self-Assessment Report - Code of Practice on Disinformation*, 2019. https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

EDIMA, *EDIMA self-assessment report on its commitments to the Code of Practice on Disinformation*, 2019. https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

ENISA, *Election cybersecurity: Challenges and opportunities*, 2019.

ENISA, *Testing cooperation of EU CSIRTs Network during large-scale cyber-attacks*, 16 May 2019. https://www.enisa.europa.eu/news/enisa-news/testing-cooperation-of-eu-csirts-network-during-large-scale-cyber-attacks.

ERGA, *ERGA Report on disinformation: Assessment of the implementation of the Code of Practice*, Brussels, 4 May 2020. https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf.

ERGA, *Report of the activities carried out to assist the European Commission in the intermediate monitoring of the Code of practice on disinformation*, Brussels, 2019. https://erga-online.eu/wp-content/uploads/2019/06/ERGA-2019-06_Report-intermediate-monitoring-Code-of-Practice-on-disinformation.pdf.

European Audiovisual Observatory, *Mapping of media literacy projects and actions in EU-28*, Strasbourg, 2016. https://ec.europa.eu/digital-single-market/en/news/reporting-media-literacy-europe.

EUvsDisinfo, *Emmanuel Macron in Russian Media*, 16 February 2017.

EUvsDisinfo, *UK, The Latest Target of Fake Russian Twitter Accounts*, 17 November 2017.

EUvsDisinfo, *5 Common Pro-Kremlin Disinformation Narratives*, 2 April 2019.

EUvsDisinfo, *EU elections update: Reaping what was sown*, 23 May 2019.

EUvsDisinfo, *European Elections: Are We Ready?*, 16 April 2019.

EUvsDisinfo, *Methods of Foreign Electoral Interference*, 2 April 2019.

EUvsDisinfo, *Russian Election Meddling and Pro-Kremlin Disinformation*, 2 April 2019.

EUvsDisinfo, 'Capitalising on the Coronavirus conspiracist frenzy', *News and Analysis*, 14 May 2020.

EUvsDisinfo, 'Conspirational virus', *News and Analysis*, 30 January 2020.

EUvsDisinfo, 'Coronavirus: the BBC challenges pro-kremlin reporting from Italy', *News and Analysis*, 1 April 2020.

EUvsDisinfo, 'Short assessment of narratives and disinformation around the Covid-19 pandemic', *EEAS Special Reports Update*, 1 April 2020.

EUvsDisinfo, 'Short assessment of narratives and disinformation around the Covid-19 pandemic', *EEAS Special Reports Update*, 1 April 2020.

EUvsDisinfo, 'Short assessment on narratives and disinformation around the Covid-19/Coronavirus pandemic', *EEAS Special Reports Update*, 24 April 2020.

EUvsDisinfo, Disinformation on the Coronavirus – Short assessment of the information environment, *EEAS Special Reports Update*, 19 March 2020.

EUvsDisinfo, 'Short assessment on narratives and disinformation around the Covid-19/Coronavirus pandemic', *EEAS Special Reports Update*, 24 April 2020.

EUvsDisinfo, 'Short assessment of narratives and disinformation around the Covid-19 pandemic', *EEAS Special Report Update*, 20 May 2020.

Facebook, *Ads about social issues, elections or politics*, Facebook for business, 2020. https://en-gb.facebook.com/business/help/167836590566506?id=288762101909005.

Facebook, *Facebook baseline report on the implementation of the Code of Practice on Disinformation*, 2018. https://ec.europa.eu/information_society/newsroom/image/document/2019-5/facebook_baseline_report_on_implementation_of_the_code_of_practice_on_disinformation_CF161D11-9A54-3E27-65D58168CAC40050_56991.pdf.

Facebook, *Facebook January 2019 Update on Implementation of the Code of Practice on Disinformation*, 2019. https://ec.europa.eu/digital-single-market/en/news/first-monthly-intermediate-results-eu-code-practice-against-disinformation.

Facebook, *Facebook February Update on Implementation of the Code of Practice on Disinformation*, 2019. https://ec.europa.eu/digital-single-market/en/news/second-monthly-intermediate-results-eu-code-practice-against-disinformation.

Facebook, *Facebook March 2019 Monthly Update on Implementation of the Code of Practice on Disinformation*, 2019. https://ec.europa.eu/digital-single-market/en/news/third-monthly-intermediate-results-eu-code-practice-against-disinformation.

Facebook, *Facebook Reports on Implementation of the Code of Practice on Disinformation – April Report*, 2019. https://ec.europa.eu/digital-single-market/en/news/fourth-intermediate-results-eu-code-practice-against-disinformation.

Facebook, *Facebook Reports on Implementation of the Code of Practice on Disinformation – May Report*, 2019. https://ec.europa.eu/digital-single-market/en/news/last-intermediate-results-eu-code-practice-against-disinformation.

Facebook, *Facebook Report on Implementation of the Code of Practice for Disinformation – Annual Report – September 2019*, 2019. https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

Gerasimov, V., *The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations*, trans. Robert Coalson, Military-Industrial Kurier, 27 February 2013.

Global Firepower, *Russia Military Strength (2020).* https://www.globalfirepower.com/country-military-strength-detail.asp?country_id=russia

GRECO, *Third Evaluation Round - Evaluation Report on Denmark on Transparency of Party Funding (Theme II)*, 29 June-2 July 2009. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806c3217.

Google, *EU Code of Practice on Disinformation – Google report*, 2018. https://ec.europa.eu/information_society/newsroom/image/document/2019-5/google_-_ec_action_plan_reporting_CF162236-E8FB-725E-C0A3D2D6CCFE678A_56994.pdf.

Google, *EC Action Plan on Disinformation – Google January Report*, 2019. https://ec.europa.eu/digital-single-market/en/news/first-monthly-intermediate-results-eu-code-practice-against-disinformation.

Google, *EC Action Plan on Disinformation – Google February Report*, 2019. https://ec.europa.eu/digital-single-market/en/news/second-monthly-intermediate-results-eu-code-practice-against-disinformation.

Google, *EC Action Plan on Disinformation – Google March Report*, 2019. https://ec.europa.eu/digital-single-market/en/news/third-monthly-intermediate-results-eu-code-practice-against-disinformation.

Google, *EC Action Plan on Disinformation – Google April Report*, 2019. https://ec.europa.eu/digital-single-market/en/news/fourth-intermediate-results-eu-code-practice-against-disinformation.

Google, *EC Action Plan on Disinformation – Google May Report*, 2019. https://ec.europa.eu/digital-single-market/en/news/last-intermediate-results-eu-code-practice-against-disinformation.

Google, *EC EU Code of Practice on Disinformation – Google annual report*, 2019. https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

Google, *Political content*, Advertising Policies Help, 2020. https://support.google.com/adspolicy/answer/6014595?hl=en.

House of Commons, Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Final Report*, London, 2019. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

IAB, *IAB Europe's self-assessment report in relation to the Code of Practice on Disinformation*, 2019. https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

Kang-Xing Jin, (2020), Facebook Newsroom: *Keeping People Safe and Informed About the Coronavirus*, 04 May 2020 https://about.fb.com/news/2020/05/coronavirus/.

Klossa, G., *Towards European Media Sovereignty*, European Commission, Brussels, 2019, https://ec.europa.eu/commission/sites/beta-political/files/guillaume_klossa_report_final.pdf.

Microsoft, *Disallowed content policies*, Advertising, 2020. https://about.ads.microsoft.com/en-us/resources/policies/disallowed-content-policies.

Microsoft, *Microsoft Self-Assessment and Report on Compliance with the EU Code of Practice on Disinformation – 1 October 2019*, 2019. https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

Mozilla, *Self-Assessment report – Code of Practice on Disinformation – September 2019*, 2019. https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

NATO. *Strasbourg / Kehl Summit Declaration*. 4 April 2009. https://www.nato.int/cps/en/natolive/news_52837.htm

NATO. *BI-SC Input for a new NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*. 25 August 2010.

https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

NATO. *EU-NATO Joint Declaration*. 8 July 2016. https://www.nato.int/cps/en/natohq/official_texts_133163.htm

NATO. *Fourth progress report on the implementation of the common set of proposals endorsed by NATO and the EU Councils on 6 December 2016 and 5 December 2017*. 17 June 2019.

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_06/190617-4th-Joint-progress-report-EU-NATO-eng.pdf

NATO (2020), Press conference, 15 Apr. 2020. https://www.nato.int/cps/en/natohq/opinions_175087.htm?selectedLocale=en

NATO (2020), Video: *How is NATO responding to disinformation on Covid-19*? 14 May 2020. https://shape.nato.int/news-archive/2020/video-how-is-nato-responding-to-disinformation-on-covid19

NIS Cooperation Group, 'Compendium on Cyber Security of Election Technology', *GC Publication*, No. 03/2018, Brussels, 2018. https://ec.europa.eu/information_society/newsroom/image/document/2018-30/election_security_compendium_00BE09F9-D2BE-5D69-9E39C5A9C81C290F_53645.pdf.

OECD, *Financing Democracy: Funding of Political Parties and Election Campaigns and the Risk of Policy Capture*, OECD Public Governance Reviews, OECD Publishing, Paris, 2016. (http://dx.doi.org/10.1787/9789264249455-en)

OSCE, *Romania Presidential Election 10 and 24 November 2019 ODIHR Election Assessment Mission Final Report*, Warsaw, 26 March 2020. https://www.osce.org/odihr/elections/romania/449200?download=true.

President of the European Council, President of the European Commission, Secretary General of the North Atlantic Treaty Organisation, Joint Declaration on EU-NATO Cooperation, 10 July 2018, https://www.nato.int/cps/en/natohq/official_texts_156626.htm

Presidente della Repubblica, Decreto-Legge 30 aprile 2019, n. 34 - Misure urgenti di crescita economica e per la risoluzione di specifiche situazioni di crisi. (19G00043) *(GU n.100 del 30-4-2019).* https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2019;34

SAR, *Implementing Code of Practice against Disinformation in Poland*, 2019. https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

SOMA, *FAQ*, 2020. https://www.disinfobservatory.org/faq/.

SOMA, *Resources*, 2020. https://www.disinfobservatory.org/resources/.

SOMA, *Observatory usage and editorial policy*, 2020. https://www.disinfobservatory.org/observatory-usage-and-editorial-policy/.

SOMA, *The Observatory*, 2020. https://www.disinfobservatory.org/the-observatory/.

Sounding Board of the Multistakeholder Forum on Disinformation Online, *The Sounding Board's unanimous opinion on the so-called Code of Practice*, 24 September 2018. https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

Twitter, *Political content*, Business, 2020. https://business.twitter.com/en/help/ads-policies/prohibited-content-policies/political-content.html.

Twitter, *Twitter progress report: Code of Practice on Disinformation*, 2018. https://ec.europa.eu/information_society/newsroom/image/document/2019-5/twitter_progress_report_on_code_of_practice_on_disinformation_CF162219-992A-B56C-06126A9E7612E13D_56993.pdf.

Twitter, *Twitter January Update: Code of Practice on Disinformation*, 2019. https://ec.europa.eu/digital-single-market/en/news/first-monthly-intermediate-results-eu-code-practice-against-disinformation.

Twitter, *Twitter February Update: Code of Practice on Disinformation*, 2019. https://ec.europa.eu/digital-single-market/en/news/second-monthly-intermediate-results-eu-code-practice-against-disinformation.

Twitter, *Twitter March Update: Code of Practice on Disinformation*, 2019. https://ec.europa.eu/digital-single-market/en/news/third-monthly-intermediate-results-eu-code-practice-against-disinformation.

Twitter, *Twitter April Update: Code of Practice on Disinformation*, 2019. https://ec.europa.eu/digital-single-market/en/news/fourth-intermediate-results-eu-code-practice-against-disinformation.

Twitter, *Twitter May Update: Code of Practice on Disinformation*, 2019. https://ec.europa.eu/digital-single-market/en/news/last-intermediate-results-eu-code-practice-against-disinformation.

Twitter, *Twitter Progress Report: Code of Practice on Disinfomration*, 2019. https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

United Nations, *Covid-19 Response: 5 ways the UN is fighting 'infodemic' of misinformation*, Department of Global Communications, 2020. https://www.un.org/en/un-coronavirus-communications-team/five-ways-united-nations-fighting-%E2%80%98infodemic%E2%80%99-misinformation

U.S. Department of Justice, Mueller, R. S., *Report on The Investigation Into Russian Interference In The 2016 Presidential Election*, Washington D.C., March 2019. https://www.justice.gov/storage/report.pdf

U.S. Department of Homeland Security, *Cybersecurity*. https://www.dhs.gov/topic/cybersecurity

WFA, *WFA Self-assessment report - Code of Practice on Disinformation*, 2019. https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019

World Health Organization. Coronavirus disease (COVID-19) advice for the public: *Myth busters*., 2020. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public/myth-busters

Articles, books and policy reports

Andreasson, L., 'Money in Politics - Why Sweden and Denmark Chose Different Paths. A Comparative Analysis of Party Finance Laws', 2019.

Australian Strategic Policy Institute, *Covid-19 disinformation and social media manipulation trends*, 17 April 2020.

Avaaz, *How Facebook can Flatten the Curve of the Coronavirus Infodemic*, 15 April 2020.

Bayer, J., 'Between Anarchy and Censorship. Public discourse and the duties of social media', *CEPS Papers in Liberty and Security in Europe*, No. 2019-03, CEPS, 2019.

Bajarūnas, E. Addressing Hybrid Threats: Priorities for the EU in 2020 and beyond. *European View*, 2020, 1-9.

Benner, T., Gaspers, J., Ohlberg, M., Poggetti, L. and Shi-Kupfer, K., *Authoritarian Advance: Responding to China's Growing Political Influence in Europe*, Global Public Policy Institute and Mercator Institute for China Studies, February 2018.

Berzina, K., Kovalcikova, N., Salvo, D., Soula, E., European *Policy Blueprint for Countering Authoritarian Interference in Democracies*, Alliance for Securing Democracy, No. 18, Washington D.C., 2019.

Berzina, K. and Soula, E., *Conceptualizing Foreign Interference in Europe*, *Alliance for Securing Democracy*, 18 March 2020.

Bradshaw, S., 'Disinformation optimised: gaming search engine algorithms to amplify junk news', *Internet Policy Review*, Vol. 8, No. 4, Alexander von Humboldt Institute for Internet and Society, 2019, p.1-24.

Brattberg, E. and T. Maurer. *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*. Carnegie Endowment for International Peace. 23 May 2018.

Brennen J., Simon F. M., Howard P., and Nielsen K., *Types, Sources, and Claims of COVID-19 Misinformation*, Reuters Institute, University of Oxford, 2020.

Bressanelli, E., *Europarties after Enlargement. Organization, Ideology and Competition*, Basingstoke, Palgrave Macmillan, 2014.

Butcher, P., *Disinformation and democracy: The home front in the information war*, European Policy Centre, 2019.

Cesarini, P., 'Disinformation during the digital era: a European code of self-discipline', *Digital Issues*, No. 6, Annales des Mines, 2019.

Christie, E.H., *Political Subversion in the Age of Social Media*, Wilfried Martens Centre, 2018.

Comai, G., 'Political funding and external interference: limits on donations, transparency, and controls', *Osservatorio Balcani e Caucaso Transeuropa*, 23 October 2019.

Corbe, M. A Collective Response to Destabilisation: The NATO Centres of Excellence. In E. Cusumano and M. Corbe (eds). *A Civil-Military Response to Hybrid Threats*. Springer International Publishing, 2017, pp. 79-100.

Cusumano E. and M. Corbe (eds). *A Civil-Military Response to Hybrid Threats*. Springer International Publishing. 2017.

Decker, B., *Adversarial Narratives: A New Model for Disinformation*, GDI, 2019.

De Maio, G., *Russia, Euroskeptic Parties, and Italian Elections*, Policy Brief, German Marshall Fund of the United States, 23 February 2018.

Dittrich, P.J., *Tackling the spread of disinformation. Why a co-regulatory approach is the right way forward for the EU*, Jacques Delors Centre – BertelsmannStiftung, 2019.

Drent, M., Hendriks, R. and D. Zandee. *New Threats, New EU and NATO Responses*. Clingendael Report. Netherlands Institute of International Relations. July 2015.

Ferro, S. and Galinyte̊, A., *Partiti e fondazioni: quanto ne sappiamo davvero dei soldi ai politici?*, Transparency International Italia, Dossier No. 1, June 2018.

Fiott, D. and R. Parkes. *Protecting Europe. The EU's response to hybrid threats*. European Union Institute for Security Studies. Chaillot papers / 151. April 2019.

Freedom House, *Beijing's Coronavirus Propaganda Has Both Foreign and Domestic Targets*, 20 April 2020.

Friends of Europe, *The dangers of the spreading 'disinformation virus'*, 28 April 2020.

Galeotti, M., *The 'Gerasimov Doctrine' and Russian Non-Linear War*, Moscow's Shadows, 2014.

Giumelli, F., Cusumano, E. and M. Besana., From Strategic Communication to Sanctions: The European Union's Approach to Hybrid Threats. In E. Cusumano and M. Corbe (eds), *A Civil-Military Response to Hybrid Threats*, Springer International Publishing, 2017, pp. 145-167

Giusti, S. and E. Piras, 'In Search of Paradigms: Disinformation, Fake News, and Post-Truth Politics'. In Giusti S. and E. Piras (Eds), *Democracy Under Attack? Disinformation, Fake News, and Post-Truth Politics*, London, Routledge, forthcoming.

Guess, A., Nagler, J., Tucker, J., 'Less than you think: Prevalence and predictors of fake news dissemination on Facebook', *Science Advances*, Vol. 5, No. 1, 2019.

Ha, M., *North Korea Turns to Cyber Disinformation Attacks Amid Global Coronavirus Outbreak*, Foundation for Defense of Democracies, 1 April 2020.

Hanon, B., *Iran's Newest Info Op Shows an Evolution of Tactics*, Alliance for Securing Democracy, 13 November 2018.

Hoffman, F. G., *Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict*, Institute for National Strategic Studies National Defence University, No. 240, April 2009.

Fagan, C., Wright, L., *Research Brief: Ad Tech Fuels Disinformation Sites in Europe – The Numbers and Players*, GDI, 2020.

Jackson, D., *Issue Brief: How disinformation impacts politics and publics*, National Endowment for Democracy, 2018.

Kalenský J.,, *Six reasons the Kremlin spreads disinformation about the coronavirus*, Atlantic Council, 24 March 2020.

Katsaitis, A., *Assessing Interest Groups' Financial Donations to the European Union's Political Parties & Foundations*, OECD Anti-corruption & Integrity Forum, 2018.

Karlsen, G. H., *Divide and rule: ten lessons about Russian political influence activities in Europe*, Palgrave, 8 February 2019.

Kello, L., *The Virtual Weapon and International Order*, Yale University Press, New Haven, 2017.

Klapsis, A., *An Unholy Alliance: The European Far Right and Putin's Russia*, Research Paper, Wilfried Martens Centre for European Studies, May 2015.

Klein, M., *Russia's Military Capabilities*, Stiftung Wissenschaft und Politik, Research Paper 2009/RP 12, October 2009.

Krasodomski-Jones, A., Smith, J., Jones, E., Judson, E., Miller, C., *Warring songs: Information operations in the digital age*, Demos, 2019.

Leerssen, P., Ausloos, J., Zarouali, B., Helberger, N., de Vreese, C.H., 'Platform ad archives: promises and pitfalls', *Internet Policy Review*, Vol. 8, No. 4, 2019, pp.1-21.

Lupion, B., *The EU Framework against disinformation: What worked, what changed and the way forward*, Democracy Reporting International, 2019.

Marchal, N., Kollanyi, B., Neudert, L.M., Howard, P.N., *Junk News During the EU Parliamentary Elections: Lessons From a Seven-Language Study of Twitter and Facebook*, Oxford Internet Institute, 2019.

McBride, J. and Chatzky, A., 'Is 'Made in China 2025' a Threat to Global Trade?', *Council on foreign Relations*, 13 May 2019.

Mcclory, J., *The Soft Power 30. A Global Renking of Soft Power*, Portland, 2018.

McGuire, M. and Dowling, S., *Cyber-crime: A review of the evidence*, Home Office, Research Report 75, Chapter 1 and 2, London, October 2013.

Melissen, J., *The New Public Diplomacy. Soft Power in International Relations*, Palgrave MacMillan, New York, 2005.

Meyer-Resende M., *Von der Leyen's Plans. What to expect from EU regulation on online threats to democracy discourse.* Briefing Paper 105. Democracy Reporting International. 2020.

Monti, M., 'La disinformazione online, la crisi del rapporto pubblico-esperti e il rischio della privatizzazione della censura nelle azioni dell'Unione Europea (Code of practice on disinformation)', in Monti, M. (ed.), *La disinformazione online e il ruolo degli esperti nell'agorà digitale: una prospettiva transdisciplinare*, No. 11/2020, Federalismi.it, 2020, p.282-305.

Nye, J.S., *Public Diplomacy and Soft Power*, The Annals of The American Academy, No. 616, March 2008. For further information.

Ohlin, J. D., *Election Interference International Law and the Future of Democracy*, Cambridge University Press, Cambridge, June 2020.

Pamment, J., 'The EU Code of Practice on Disinformation: Briefing note for the new EU Commission', *Policy Perspectives Series*, Carnegie Endowment for International Peace: Partnership for countering influence operations, 2020.

Polyakova, A., Kounalakis, M., Klapsis, A., Germani, L.S., Iacoboni, J., de Borja Lasheras, F. and de Pedro, N., *The Kremlin's Trojan Horses 2.0: Russian Influence in Greece, Italy, and Spain*, Eurasia Center, Atlantic Council, November 2017, pp. 14-18.

Polyakova, A., Fried, D., *Democratic Defense Against Disinformation 2.0*, Atlantic Council, 2019.

Pomerantsev, P. and Weiss, M., *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, Institute of Modern Russia, New York, 2014.

ProPublica, *How China Built a Twitter Propaganda Machine Then Let It Loose on Coronavirus*, 26 March 2020.

Rieder, B., Matamoros-Fernandez, A., Coromina, O., 'From ranking algorithms to "ranking cultures": Investigating the modulation of visibility in YouTube search results', *International Journal of Research into New Media Technologies*, Vol. 24, No. 1, 2018, p.50-68.

Rugge, F., *Cybercrime and international relations*, Istituto per gli Studi di Politica Internazionale (ISPI), 16 July 2018.

Rühlig, T. N., Jerdén, B., van der Putten, F., Seaman, J., Otero-Iglesias, M., Ekman, A., *Political values in Europe-China relations*, European Think-tank Network on China (ETNC) Report, December 2018.

Sawiris, M, Dušková, L., Syrovátka, J., Győri, L., *European elections in Central Europe: Information operations and disinformation campaigns*, GLOBSEC, National Endowment for Democracy, 2019.

Sawiris, M, Dušková, L., Syrovátka, J., Győri, L., Wierzejski, A., *European elections in the V4*, GLOBSEC, National Endowment for Democracy, 2019.

Shekhovtsov, A., *Russia and the Western far right: Tango Noir*. New York, Routledge, 2018.

Syrovátka, J., 'In Scrooge's boots: Lessons learned on disinformation from the 2019 European elections', *European view*, Vol. 18, No. 2, 2019, p.203-209.

Sperling, J., The European Union and the grand security strategy for post-Westphalian governance. In S. Economides and J. Sperling (eds). *EU Security Strategies. Extending the EU System of Security Governance*. Routledge, 2018, pp. 1-25.

Snegovaya, M., *Putin's Information Warfare In Ukraine. Soviet Origins Of Russia's Hybrid Warfare*, Institute for the Study of War, Russia Report I, Washington, September 2015.

Svárovský, M., Janda, J., Víchová, V., Gurney, J. and Kröger, S., *Handbook On Countering Russian And Chinese Interference In Europe*, European Values Center For Security Policy, 2019.

Szicherle, P., Lelonek, A., Mesežnikov, G., Syrovátka, J, Štěpánek, N., *Investigating Russia's role and the Kremlin's interference in the 2019 EP elections*, Friedrich Naumann Foundation, Political Capital, 2019.

Tanner, M., *Economic Coercion: Factors Affecting Success and Failure. In Chinese Economic Coercion Against Taiwan: A Tricky Weapon to Use*, Rand Corporation, Santa Monica, 2017, pp. 11-32.

Tucker, J. A., Guess, A., Barberá, P., Vaccari, C., Siegel, A., Sanovich Stukal, S. and Nyhan, B., *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*, Hewlett Foundatio, March 2018, p. 51.

Tzu, S., *The Art of War*, Shambhala Publications, London, 1988, Chapter 1.

Vilmer, J.B.J., *Successfully Countering Russian Electoral Interference*, CSIS, 2018.

Wagnsson C. and M. Hellman, Normative Power Europe Caving in? EU under Pressure of Russian Information Warfare, *Journal of Common Market Studies*, Vol 56, No 5, 2018, pp. 1161-77.

Journalistic sources and blogs

Aiossa, N., *3 ways MEPs can fiddle expenses*, Transparency International, 27 January 2017.

Alandete, A. and Verdú, D., 'How Russian networks worked to boost the far right in Italy', *El País*, 1 March 2018.

Alandete, D., 'How the Russian meddling machine won the online battle of the illegal referendum', *El País*, 13 November 2017.

Alandete, D., 'Pro-Russian networks see 2,000% increase in activity in favor of Catalan referendum', *El País*, 01 October 2017.

Alandete, D., 'Russian network used Venezuelan accounts to deepen Catalan crisis', *El País*, 11 November 2017.

Apuzzo, M., 'Europe Built a System to Fight Russian Meddling. It's Struggling', *New York Times*, 6 July 2019.

Apuzzo M., 'Pressured by China, E.U. Softens Report on Covid-19 Disinformation', *The New York Times*, 24 April 2020.

Barnes J., Rosenberg M., Wong E., 'As Virus Spreads, China and Russia See Openings for Disinformation', *The New York Times*, 28 March 2020.

BBC News, 'France's Marine Le Pen urges end to Russia sanctions', 24 March 2017.

BBC News, 'Austrian far-right FPÖ quits Kurz government after sacking', 21 May 2019.

BBC News, 'German AfD leader Petry meets pro-Putin Russian MPs', 21 February 2017

Beauchamp, Z., *The key findings from the US intelligence report on the Russia hack, decoded*, Vox, 6 January 2017.

Beaumont P., Borger J., Boffey D., 'Malicious forces creating 'perfect storm' of coronavirus disinformation', *The Guardian*, 24 April 2020.

Bechis F., 'Infodemia, chi vince? I numeri di Swg e il dibattito al Centro Studi Americani', *Formiche.net*, 05 May 2020.

Bell, B., 'Austria scandal: Mystery of the honey-trap video', *BBC News*, 24 May 2019.

Bond, D. and Fildes, N., *UK Intelligence Panel Warns on Huawei Security Flaws*, Financial Times, 28 March 2019.

Cadwalladr, C., 'Arron Banks, Brexit and the Russia connection', *The Guardian*, 16 June 2018.

Cadwalladr, C., 'The great British Brexit robbery: how our democracy was hijacked', *The Guardian*, 7 May 2017.

Cellan-Jones. R., 'Facebook and Twitter: Nine Russian Brexit ads found by inquiries, *BBC News*, 13 December 2017.

Child D., 'Fighting fake news: The new front in the coronavirus battle', *Aljazeera*, 13 April 2020.

Crawford, A., *Assessing North Korea's Cyber Evolution*, Divergent Options, 25 November 2019.

Culliford E., 'Twitter opens up data for researchers to study Covid-19 tweets', *Reuters*, 29 April 2020.

Decker, B., *Adversarial Narratives: A New Model for Disinformation*, Global Disinformation Index, August 2019.

Dempsey J., *Judy Asks: Is the Coronavirus Breeding Disinformation Across Europe?*, Judy Dempsey's Strategic Europe, Carnegie Endowment for International Peace, 09 April 2020.

Deutsche Welle, 'Head of the AfD Frauke Petry meets with Russian officials in Moscow', 20 February 2017.

Deutsche Welle, *EU elections: Commissioner warns of Russian meddling*, 13 May 2019.

Díez, A. and Mateo, J.J., 'Government confirms intervention of Russian hackers in Catalan crisis', *El País*, 10 November 2017.

DutchNews, 'PVV hardest hit as government bans non-EU political donations', 25 January 2019.

Efremov, S., *The Challenges of Russia's Economy: An Overview*, Istituto per gli Studi di Politica Internazionale, 4 November 2019.

Euractiv, 'Whistleblower: Cambridge Analytica Shared Data with Russia.' 17 May 2018.

Faucon, B., *Iran Leverages Oil to Court Other U.S. Rivals During Pandemic*, The Wall Street Journal, 11 May 2020.

Frye, T., *Putin touts Russia as a great power. But he's made it a weak one*, Washington Post, 6 June 2019.

Gatehouse, G., 'Marine Le Pen: Who's funding France's far right?', *BBC News*, 3 April 2017.

Gessant *C.* M. 'Borrell rejette les allégations de modification d'un rapport sur la désinformation', à la suite de pressions chinoises', *Agence Europe*, Brussels, 30 April 2020.

Henley, J., 'EU watchdog asks Marine Le Pen to repay €339,000 in staff salaries', *The Guardian*, 31 October 2016.

Hern, A., 'Macron hackers linked to Russian-affiliated group behind US attack', *The Guardian*, 8 May 2017.

Hern A., 'Twitter to remove harmful fake news about coronavirus', *The Guardian*, 19 March 2020.

Hern A., 'WhatsApp to impose new limit on forwarding to fight fake news', *The Guardian*, 07 April 2020.

Higgins, A., 'Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote', *The New York Times*, 16 February 2017.

Horowitz, J., 'Steve Bannon's "Movement" Enlists Italy's Most Powerful Politician', *The New York Times*, 7 September 2018.

Jacobsen, H., 'European Parliament tells MEP to return €400,000', *Euractiv*, 6 May 2016

Karnitschnig, M., 'Austrian government collapses over Russia scandal', *Politico*, 18 May 2019.

Kayali, L. and de la Baume, M., 'EU on Facebook ad rules', *Politico*, 16 April 2019.

Kergueno, R., *Fraud and boats: funding European political parties*, Transparency International EU, 9 November 2017.

Khan, M., 'EU targets European political parties that misuse voters' data', *Financial Times*, 26 August 2018.

Klasa, A., Hopkins, V., Chazan, G., Foy, H. and Johnson, M., 'Russia's long arm reaches to the right in Europe', *Financial Times*, 23 May 2019.

Kroet, C.**,** 'Dutch ban on foreign funding for political parties would hit far-right PVV', *Politico*, 1 January 2018.

Kurlantzick, J., 'As China Extends Its Reach Abroad, When Does Influence Become Interference?', *World Politics Review*, 8 January 2018.

Le Blond. J., 'German politicians' personal data leaked online', *The Guardian*, 4 January 2019.

Medium, '#ElectionWatch: Disinformation in Deutschland', 28 September 2017.

Menn, J., 'Exclusive: Russia used Facebook to try to spy on Macron campaign – sources', *Reuters*, 27 July 2017.

Meister, S., 'The "Lisa case": Germany as a target of Russian disinformation', *NATO Review*, 25 July 2016.

Mohdin, A., 'The Dutch far right's election donors are almost exclusively American', *Quartz*, 10 March 2017.

Murphy, F. and Osborn, A., 'Austrian far right signs deal with Putin's party, touts Trump ties', *Reuters*, 19

Nardelli, A., 'Revealed: The Explosive Secret Recording That Shows How Russia Tried To Funnel Millions To The "European Trump"', *BuzzFeed News*, 10 July 2019.

Oliveira, I., 'National Front seeks Russian cash for election fight', *Politico*, 19 February 2016.

Pop V., 'EU, Tech Firms Renew Pact to Fight Coronavirus Disinformation', *The Wall Street Journal*, 11 March 2020.

Rankin, J. and Lewis, P., 'Bannon's Europe plan: a look at the law in his 13 targeted countries', *The Guardian*, 21 November 2018.

Rankin, J., 'Defunct Eurosceptic party linked to Ukip asked to repay €1.1m', *The Guardian*, 30 May 2018.

Reid, A., Waldman, A., *Viral 'Rigged' Voting Machine Video Actually User Error*, Electionland, 8 November 2016.

Rettman, A. 'Mogherini urged to do more on Russian propaganda', *EUObserver*, 20 October 2017.

Rettman, A., 'WhatsApp leak exposes Russia link to Dutch far right', *EuObserver*, 17 April 2020.

Rogers, K., Bromwich, J. E., *The Hoaxes, Fake News and Misinformation We Saw on Election Day*, *New York Times*, New York, 11 September 2016.

Rubin, A.J., 'Geert Wilders, Reclusive Provocateur, Rises Before Dutch Vote', *The New York Times*, 27 February 2017.

Sanger, D. E, Kirkpatrick, D. D. and Perlroth, N., The World Once Laughed at North Korean Cyberpower. No More, New York Times, 15 October 2017.

Schaart, E., 'Dutch far-right leader Baudet had ties to Russia, report says', *Politico*, 17 April 2020.

Shane, S., Mazzetti, M., *The Plot to Subvert an Election*, The New York Times, 20 September 2018.

Schmidt, R., 'Russia, the far right, and anti-Macron bots', *EuObserver*, 3 May 2017.

Schenk, M., BREAKING: Dutch Parliament Approves Motion Calling To Disband EUvsDisinfo, *LeadStories*, 6 March 2018.

Seddon, M. and Politi, J., 'Putin's party signs deal with Italy's far-right Lega Nord', *Financial Times*, 6

Shuster, S., 'How Russian Voters Fueled the Rise of Germany's Far-Right', *TIME*, 25 September 2017.

Sloan, A. and Campbell, I., 'How did Arron Banks afford Brexit?', *OpenDemocracy*, 19 October 2017.

Smith, D., 'WikiLeaks emails: what they revealed about the Clinton campaign's mechanics', *The Guardian*, 6 November 2016.

Speranza, L., '#ElectionWatch: How Russia-Italy Relations are Impacting the Italian Elections', *New Atlanticist Blog*, 3 March 2018.

Spring M., 'Coronavirus: Viral WhatsApp messages 'drop 70%'', *BBC News*, 27 April 2020.

Stolton, S.,' EU Commission takes aim at disinformation, admits funding deficit', *Euractiv*, 6 December 2018.

Stolton, S. 'Media freedom and pluralism 'key' to Democracy Action Plan', *Euractiv*, 3 March 2020.

Stolton S., 'EU Rapid Alert System used amid coronavirus disinformation campaign', *Euractiv*, 10 March 2020.

Stolton S., 'Regulation against fake news 'very important,' Reynders says', *Euractiv*, 15 April 2020.

Timberg C., 'On Twitter, almost 60 percent of false claims about coronavirus remain online-without a warning label', *The Washington Post*, 08 April 2020.

The Local, 'Denmark agrees law against "antidemocratic" foreign donations', 3 May 2019.

Tizian, G. and Vergine, S., 'Quei 3 milioni russi per Matteo Salvini: ecco l'inchiesta che fa tremare la Lega', *L'Espresso*, 21 February 2019.

Woodruff Swan B., 'State report: Russian, Chinese and Iranian disinformation narratives echo one another', *Politico*, 21 April 2020.

Za, V., 'Facebook takes down fake Italian accounts ahead of EU election', *Reuters*, 12 May 2019.

ANNEXES

ANNEX 1. NATO CENTRES OF EXCELLENCE: PARTICIPATION BY MEMBER STATE

EU 27 Member	EU/NATO Hybrid CoE	NATO StratCom CoE	NATO Cyber Defence CoE
Austria	Participating		Participating
Belgium			Participating
Bulgaria			Participating
Cyprus	Participating		
Croatia			
Czech Republic	Participating		Participating
Denmark	Participating		Participating
Estonia	Participating	Participating	Participating
Finland	Participating		Participating
France	Participating	Finalising entry	Participating
Germany	Participating	Participating	Participating
Greece	Participating		Participating
Hungary	Participating		Participating
Ireland			
Italy	Participating	Participating	Participating
Latvia	Participating	Participating	Participating
Lithuania	Participating	Participating	Participating
Luxembourg	Participating		
Malta			
Netherlands	Participating		Participating
Poland	Participating	Participating	Participating
Portugal	Participating		Participating
Romania	Participating		Participating
Slovakia		Finalising entry	Participating
Slovenia	Participating		
Spain	Participating		Participating
Sweden	Participating		Participating

Sources: As of 24 April 2020. Sources: ; Hybrid CoE; NATO StratCom CoE; Nato Cyber Defence CoE

ANNEX 2: THE EP'S RESOLUTION ON FOREIGN ELECTORAL INTERFERENCE

The EP's demands	Addressee	Responses
Include specific courses on media literacy in their school curricula and develop information campaigns	MS Commission	Creative Europe programme, Erasmus + Digital Education Acrion Plan update (to be adopted in late 2020)
Strive to increase the EU's capabilities in IT and hardware	Council Commission	European strategy for data Digital Europe programme
Create an innovation friendly environment	Commission MS	Digital Services Act
Support responsible journalism and public service media	Council Commission	Media freedom projects[343]
Support democratic, independent and diverse media in the countries of the EU Neighbourhood	Council Commission	Media freedom projects
Upgrade of the EU East StratCom Task Force to a permanent structure within the EEAS with significantly higher financing and staffing levels	Council EEAS	
Classify electoral equipment as critical infrastructure so as to ensure that in the event of a breach NIS directive responses can be applied	Commission	Review of the NIS Directive (last Q of 2020)
Call for investigations into alleged illegal use of the online political space by foreign forces	MS supported by Eurojust	
Continue monitoring of the impact of foreign interference across Europe	Commission EEAS	East StratCom Task Force EUvsDisinfo EDMO set up in June 2020[344]
Make the fight against disinformation a central foreign policy objective	VP-HR	VP-HR Borrell, opening statement before the EP, 30.04.20[345]

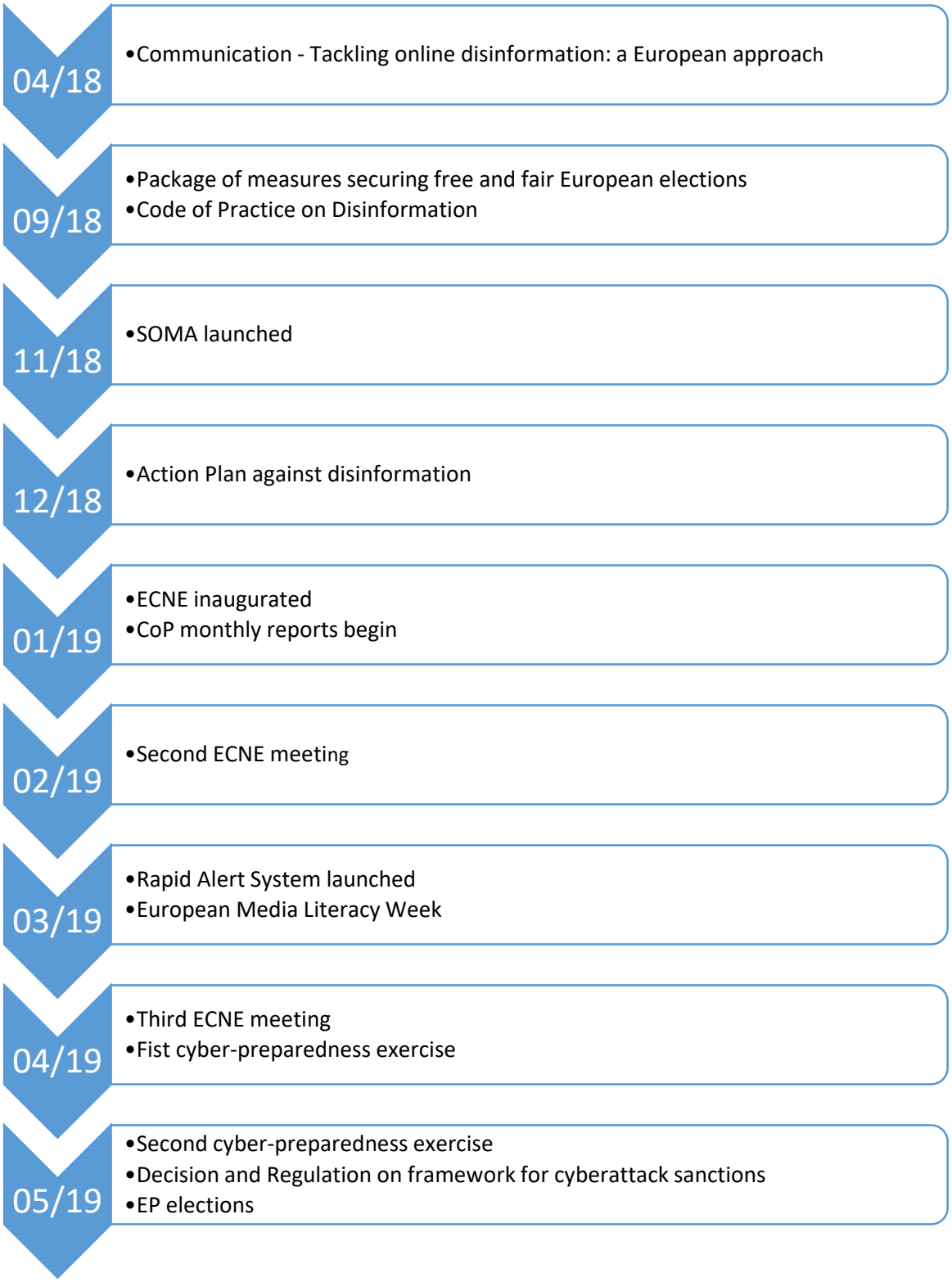
[343] European Commission, *Media Freedom Projects*, 2 March 2020.
[344] European Commission, *Daily News*. 5 May 2020.
[345] European External Action Service, *Disinformation around the coronavirus pandemic: Opening statement by the HR/VP Josep Borrell at the European Parliament*, 30 April 2020.

		New Security Union Strategy[346]
Evaluate legislative and non-legislative actions which can result in interventions by social media platforms	Commission	Legislative proposal on paid political advertising Reform of the Code of Practice on Disinformation European Democracy Action Plan Digital Services Act
Support public institutions, think-tanks, NGOs, and grassroots cyber-activists working on issues of propaganda and disinformation	Commission MS	European Democracy Action Plan EDMO set up in June 2020
Make funding and support available for public awareness-raising campaigns aimed at increasing citizens' resilience on disinformation	Commission MS	European Democracy Action Plan
Establish and disseminate a policy on whistle-blowing	Council of Europe MS	Discussion on the establishment of a convention on the protection of whistle blowers[347]
Engage in discussion with stakeholders as well as international partners to step actions to counter hybrid threats	Commission MS	Ongoing discussions with stakeholders and international partners
Address the issue of foreign funding of European political parties and foundations	Commission	European Democracy Action Plan Legislative proposal on the financing of European political parties

[346] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, *Joint communication to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions. Tackling COVID-19 disinformation - Getting the facts right*, JOIN(2020) 8 final. Brussels, 10 June 2020.

[347] Council of Europe, *Improving the protection of whistle-blowers all over Europe*, Reply to recommendation. Doc. 15099, 29 April 2020.

ANNEX 3. TIMELINE OF EU MEASURES PREPARING FOR THE 2019 EP ELECTIONS



Source : Own elaboration.

ANNEX 4. PLATFORMS' ONLINE SAFETY AND MEDIA LITERACY PROJECTS IN 2017-19

	Projects
Facebook	Cooperation with Full Fact (UK), Maldita (ES), Newtral (ES), Correctiv (DE), TheJournal (IE), Pagella Politica (IT), Demagog (CZ), Nieuwscheckers (NL) and Ellinika Hoaxes (GR) to launch a media literacu campaign in all Member States on false news. Cooperation with Freeformers and over 20 in-country NGOs and training organizations to deliver a Digital Skills Training Programme to 75,000 citizens across seven European countries (Italy, Germany, Spain, Poland, the UK and Ireland). Digital Literacy Library: collection of online lessons to help young people think critically and share thoughtfully online. EC partnership for the EU Media Literacy Week in Brussels. EU Elections training programme for candidates, parties and political advertisers. EU elections integrity campaign for awareness-raising across the EU. Facebook Journalism Project: trainings for journalists on online safety, news integrity and use of platforms. Partnership with EAVI (Media Literacy for Citizenship) and the European Youth Forum to participate to Yo!Fest 2019, a political youth festival on elections and democracy. Denmark: • Digital Literacy Day debates for young first-time voters. France: • Cooperation with 12 civic projects funded through the Fund for Online Civility. Germany: • Cooperation with Zeit für die Schule to increase students' media literacy. • Cooperation with Digibits to increase students' media literacy. Italy: • Cooperation with institutions and industry actors to work on the media literacy campaign '#BastaBufale' (StopHoaxes). • Partnership with Freeformers on the Future Worforce Model. • Partnership with Fondazione Mondo Digitale on students' and elderly's media literacy. Ireland: • Cooperation with Media Literacy Ireland and the Broadcasting Authority of Ireland for the 'Be Media Smart' awareness campaign, targeted at people of all ages. Poland: • Cooperation with Polityka Insight and Press to work on the media literacy campaign 'Learning to read in the false news era'. • Cooperation with the Digital Youth Forum to organise a three-day educational event for young people. • Newsrooms training. Portugal:

	• Partnership with DGE, SeguraNet, Centro de Internet Segura and FCT for the GeraZão project on young people's media literacy. UK: • Funding for the National Literacy Trust's Commission on Fake News and the Teaching of Critical Literacy Skills in Schools.
Google	Cooperation with several NGOs for the 'Be Internet awesome' and 'Be Internet Citizens' campaigns aimed at media literacy respectively for children and teenagers, as well as their parents and educators. Cooperation with the IFCN (International Fact Checking Network) to launch the collaborative fact-checking platform 'FactCheckEU'. Global Media Literacy Summit to build a network of media literacy practictioners. Research and reporting trainings for journalists. Security trainings for election-involved officials, journalists and NGOs. Support to First Draft to train journalists to use CrossCheck, a knowledge sharing platform. Czech Republic: • Support to 'One World at Schools' to promote students' media literacy. Finland: • Support to The Mannerheim League for Child Welfare and Save the Children. France: • Support to e-Enfance for school trainings through 'Be Internet awesome'. Portugal: • Support to the Portuguese Press Association for media literacy projects aimed at young and elderly people and at professionals. Spain: • Cooperation with the FDA Foundation, state institutions and all main media groups to launch '(In)fòrmate', aimed at students' media literacy. UK: • Support to The Student View to promote students' media literacy.
Twitter	Contribution to the EU Media Literacy Week and the Democracy Alive festival. '#HerStory' initiative for World Press Freedom Day. Partnership with UNESCO to promote Global Media and Information Literacy Week and to produce the 'Teaching and Learning with Twitter' guide for educators. Production of the 'Educator's Guide to Twitter'. Support to 10 NGOs in the UNESCO's media and literacy network. Support to Twitter's safety partners for Safer Internet Day 2019. Support to the Alliance of Democracies on election integrity and to the '#WeDeserveBetter' campaign, focusing on hate speech. Trainings for EU parties, EU officials and national parties and officials across the EU on safety and security. France: • Partnership with CLEMI students.

	Ireland: • Support to the 'BeMediaSmart' campaign from Media Literacy Ireland, aimed at people of all ages. • Cooperation with the Department of Communications, Climate Action and Environment in the School Digital Champions programme for students. UK: • Support to Shout Out UK and Bite the Ballot for young peoples' media literacy programmes. • 'Tea, Toast and Tweeting' session on digital literacy for over 50s.
Microsoft	Support to NewsGuard's digital media literacy program.

Source: Own elaboration from the CoP signatories' reports and the ERGA assessment report.

ANNEX 5. LIST OF DISINFORMATION-RELATED PROJECTS (H-2020 AND FP-7)

Project	EU Contribution	Topic/aim	Leading country	Period
SocialSensor	EUR 6 500 000	Improved media search	LU	2013-2016
Reveal	EUR 5 100 000	Evaluation of Information trustworthiness	LU	2013-2016
Comprop	EUR 2 000 000	Impact of bots and algorithms on political debates	UK	2016-2020
Botfind	EUR 150 000	Bot's effectiveness in information operations	UK	2017-2019
Debunker	EUR 2 000 000	Solutions to information misperceptions	UK	2016-2020
ELHO	EUR 2 500 000	Causes of electoral hostility	UK	2019-2024
GoodNews	EUR 150 000	Fake news detection through deep learning	CH	2018-2020
Invid	EUR 3 100 000	Development of video verification tools	GR	2016-2018
Fandango	EUR 2 900 000	False news detection through big data analysis	IT	2018-2020
Co-creating Misinformation	EUR 4 100 000	Misinformation analysis and development of countermeasures	SW	2018-2021
Eunomia	EUR 2 500 000	Decentralised verification and trust-rating tools	UK	2018-2021
SocialTruth	EUR 2 500 000	Verification system for different verification services	GR	2018-2021
Provenance	EUR 2 500 000	Content verification	IE	2018-2021
WeVerify	EUR 2 500 000	False content detection through a multimodal approach	BG	2018-2021

Source: Klossa, G., *Towards European Media Sovereignty*, European Commission, 2019, p.85-90; Horizon 2020 funded projects, available at https://data.europa.eu/euodp/en/data/dataset/cordisH2020projects/resource/010f269b-9ee3-45a0-afea-c43aa1ef61ac. Note: the SOMA project is not included in this list.

ANNEX 6: BANS ON FOREIGN DONATIONS TO POLITICAL PARTIES

Country	1. Is there a ban on donations from foreign interests to political parties?	Details
Austria	No	Donations from foreign natural or legal persons must not exceed EUR 2 500.
Belgium	No	Absent from laws/unregulated. However, all donations by legal persons are prohibited.
Bulgaria	Yes	
Croatia	Yes	
Cyprus	Yes	Private donations above EUR 5 000/year are only allowed from natural persons with Cypriot nationality or Cypriot origins or from legal persons having the permanent residence in the Republic.
Czech Republic	Yes	
Denmark	No	
Estonia	Yes	Donations by aliens are prohibited, except for persons holding the permanent right of residence or the status of long-term resident in Estonia.
Finland	Yes	However, a party may receive foreign contributions from individuals and international associations and foundations that represent the party's ideological attitude.
France	Yes	However, foreign individuals residing in France can contribute to a campaign or donate money to a political party.
Germany	No	There is however a limit on how much foreigners may contribute which is EUR 1 000.
Greece	No	Although foreign sources are not specifically mentioned, the law bans donations and services from natural persons/not Greek nationals, public legal entities or private entities, local authorities at every level, natural persons/owners (their spouses and descendants) of journals, radio and TV channels.
Hungary	Yes	The Law on Party Finance of Hungary prohibits donations from companies and foreign individuals or organizations.

Ireland	Yes	
Italy	Yes	Parties are banned from receiving foreign donations. Only foundations and associations can receive foreign donations, but they aren't allowed to redirect them to political parties.
Latvia	Yes	Only citizens and persons who have the right to receive an Aliens passport of the Republic of Latvia are allowed to make donations for political parties.
Lithuania	Yes	However, permanent residents holding the citizenship of any other EU Member State can be donors to political parties or candidates of campaigns for European Parliament elections and municipal councils.
Luxembourg	No	
Malta	Yes	There is a ban on foreign donation, but exceptions could be made.
Netherlands	No	
Poland	Yes	Political parties may not accept funds originating from natural persons with no place of residence in the Republic of Poland (with the exception of Polish citizens living abroad), and foreigners albeit having a place of residence in Poland.
Portugal	Yes	
Romania	Yes	
Slovakia	Yes	Political parties may not accept donations and other gratuitous services from associations of municipalities and organizations with an international element.
Slovenia	Yes	Political parties cannot acquire funds from contributions of foreign private citizens, legal entities and natural persons, or from party's property incomings from abroad, from bequests and gifts from abroad, or to acquire funds or perform services for a party from abroad.
Spain	Yes	Political parties can accept donations from foreign natural persons, within the limits provided by the law for private donations. However, they are not allowed to receive donations from foreign governments, foreign entities or public companies, or companies which are directly linked to the parties.
Sweden	No	

United Kingdom	Yes	

Source: International IDEA.

ANNEX 7: BANS ON FOREIGN DONATIONS TO CANDIDATES

Country	2. Is there a ban on donations from foreign interests to candidates?	Details
Austria	No	Donations from foreign natural or legal persons must not exceed EUR 2 500.
Belgium	No	Absent from laws/unregulated. However, all donations by legal persons are prohibited.
Bulgaria	Yes	
Croatia	Yes	
Cyprus	No	
Czech Republic	Yes	Although there is no clear indication, only registered third parties can make donations to candidates; foreign legal persons and natural persons who are not citizens of the Czech Republic cannot be registered as third parties.
Denmark	No	
Estonia	Yes	Donations by aliens are prohibited, except for persons holding the permanent right of residence or the status of long-term resident in Estonia.
Finland	Yes	However, a candidate may receive foreign contributions for the election campaign from individuals and international associations and foundations that represent the candidate's ideological views.
France	Yes	However, foreign individuals residing in France can contribute to a campaign or donate money to a political party.
Germany	No	Party members who receive donations on behalf of their party shall immediately pass them onto the party administration.
Greece	No	Although foreign sources are not specifically mentioned, the law bans donations and services from natural persons/not Greek nationals, public legal entities or private entities, local authorities at every level, natural persons/owners (their spouses and descendants) of journals, radio and TV channels.

Hungary	Yes	The Law on Party Finance of Hungary prohibits donations from companies and foreign individuals or organizations to both parties and candidates.
Ireland	Yes	
Italy	Yes	Candidates are banned from receiving foreign donations. Only foundations and associations can receive foreign donations, but they aren't allowed to redirect them to candidates.
Latvia	Yes	All financial activities by a candidate are considered as financial activities of his/her respective nominating political party.
Lithuania	Yes	However, permanent residents holding the citizenship of any other EU Member State can be donors to political parties or candidates of campaigns for European Parliament elections and municipal councils.
Luxembourg	No	
Malta	Yes	There is a ban on foreign donation, but exceptions could be made.
Netherlands	No	
Poland	Yes	The financial resources of the election committee for the candidate for President of the Republic can only come from the contributions of Polish citizens with permanent domicile in the Polish Republic, and the election funds of political parties and bank loans taken out for purposes related to elections.
Portugal	Yes	
Romania	Yes	
Slovakia	Yes	The presidential candidate and independent candidates may not accept donations or any other gratuitous service for the election campaign from associations of municipalities and organizations with an international element.
Slovenia	Yes	
Spain	No	The present legislation covers political parties and not candidates.
Sweden	No	

United Kingdom	Yes	Donations to candidates largely follow the same rules as to political parties: contributions to candidates below GBP 50 can be anonymous and can therefore be made by foreign interests.

Source: International IDEA.

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the AFCO Committee, assesses the EU responses to counter foreign interferences. It examines in particular the effectiveness of the EU action against foreign interferences in the 2019 European Parliament elections, the COVID-19 crisis and the issue of foreign donations to European political parties. The study concludes with specific policy recommendations to enhance the EU's responses.

PE 655.290
IP/C/AFCO/IC/2020-035

Print ISBN 978-92-846-6887-8 | doi:10.2861/345170 | QA-02-20-514-EN-C
PDF ISBN 978-92-846-6886-1| doi:10.2861/773020 | QA-02-20-514-EN-N