STUDY

Requested by the Authority for European Political Parties and European Political Foundations

Autorité pour les partis politiques européens et les fondations politiques européennes

# Foreign Electoral Interference Affecting EU Democratic Processes

Autorité pour les partis politiques européens et les fondations politiques européennes

Authority for European Political Parties and European Political Foundations - November 2023

# Foreign Electoral Interference Affecting EU Democratic Processes

**Abstract**

Malign foreign state and non-state actors employ intricate strategies to manipulate elections, including in Europe. This study sets out the toolbox of malign actors affecting the EU. It delves into financial incentives, information manipulation, and cyber interventions, all while spotlighting Russia and China's roles.

Autorité pour les partis politiques européens et les fondations politiques européennes

This document was requested by the Authority for European Political Parties and European Political Foundations.

**AUTHORS**
Ivana KARÁSKOVÁ, Association for International Affairs (AMO)
Una Aleksandra BĒRZINA-ČERENKOVA, Association for International Affairs (AMO)
Kara NĚMEČKOVÁ, Association for International Affairs (AMO)

**LINGUISTIC VERSIONS**
Original: EN

Manuscript completed in August 2023.


This document is available on the internet at:
https://www.appf.europa.eu/appf/en/other-information/studies

**DISCLAIMER AND COPYRIGHT**

# CONTENTS

**LIST OF ABBREVIATIONS** **4**

**LIST OF BOXES** **6**

**1. INTRODUCTION** **9**

**2. HOW MALIGN FOREIGN ACTORS INFLUENCE ELECTIONS** **17**

2.1. Financial interference 17

2.1.1. Background 17

2.1.2. Methods 19

2.1.3. Reflection 29

2.2. Information Manipulation 30

2.2.1. Background 30

2.2.2. Methods 32

2.2.3. Reflection 43

2.3. Cyber-enabled electoral interference 45

2.3.1. Background 45

2.3.2. Methods 48

2.3.3. Targets 50

2.3.4. Perpetrators 52

2.3.5. Reflection 57

**3. CONCLUSION** **60**

# LIST OF ABBREVIATIONS

| | |
|---|---|
| **AI** | Artificial Intelligence |
| **AIVD** | General Intelligence and Security Service (Netherlands) |
| **APPF** | Authority for European Political Parties and European Political Foundations |
| **APT** | Advanced Persistent Threat |
| **ASP** | Social Design Agency |
| **ASPI** | Australian Strategic Policy Institute |
| **BRI** | Belt and Road Initiative |
| **CCP** | Chinese Communist Party |
| **CDU** | Christian Democratic Union of Germany |
| **CEO** | Chief Executive Officer |
| **CFO** | Chief Financial Officer |
| **COVID-19** | Coronavirus pandemic of 2019 |
| **CRRTs** | Cyber Rapid Response Teams |
| **CSIS** | Canadian Security Intelligence Service |
| **DGAP** | German Council on Foreign Relations |
| **DNC** | Democratic National Committee (United States) |
| **DCCC** | Democratic Congressional Campaign Committee (United States) |
| **DPP** | Democratic Progressive Party (Taiwan) |
| **DoS** | Denial-of-Service attacks |
| **DDoS** | Distributed Denial-of-Service attacks |
| **ENISA** | European Union Agency for Cybersecurity |

| | |
|---|---|
| **EU** | European Union |
| **EURATOM** | European Atomic Energy Community |
| **FBI** | Federal Bureau of Investigation (United States) |
| **GRU** | Glavnoye Razvedyvatelnoye Upravlenie/Chief Intelligence Office (Russia) |
| **ICT** | Information and Communication Technology |
| **KMT** | Kuomintang |
| **KGB** | Komitet gosudarstvennoy bezopasnosti/Committee for State Security (USSR) |
| **MP** | Member of Parliament |
| **MSTIC** | Microsoft's Threat Intelligence Center |
| **NATO** | North Atlantic Treaty Organization |
| **NSCS** | National Cyber Security Center (United Kingdom) |
| **PESCO** | Permanent Structured Cooperation |
| **PRC** | People's Republic of China |
| **RRN** | Reliable Russian News |
| **SLAPP** | Strategic Lawsuit Against Public Participation |
| **SMEs** | Small and medium-sized enterprises |
| **SVR** | Sluzhba vneshney razvedki/Foreign Intelligence Service (Russia) |
| **TAG** | Google Threat Analysis Group |
| **TTPs** | Tactics, techniques and procedures |
| **UK** | United Kingdom |
| **US** | United States |
| **USSR** | Union of Soviet Socialist Republics |
| **VIGINUM** | Vigilance and Protection against Foreign Interference (France) |

# LIST OF BOXES

Box 1: Exchanging financial contributions for shifts in stance on South China Sea 24
Box 2: Using WeChat to recruit a candidate acceptable to China 27
Box 3: The RRN Case as an example of typosquatting 33
Box 4: The META Czech case 35
Box 5: The case of COVID-19 origins 38
Box 6: The Vystrčil case 40
Box 7: The Zhenhua Data Information Technology case 41
Box 8: Putin's People case 43
Box 9: Russian attempts to meddle in the 2021 German elections 49

# EXECUTIVE SUMMARY

## Background

The Authority for European Political Parties and European Political Foundations (APPF) contracted the Association for International Affairs (AMO) on 31 March 2023 to prepare a study on foreign interference tools capable of harming EU democratic processes.

## Aim of the study

- to identify and provide a comprehensive picture of the toolbox used by malign non-EU actors to influence and interfere with democratic processes inside the European Union, with a focus on the European electoral context (including the run-up and aftermath of the actual 2024 European elections) but not limited thereto. The scope of the malign toolbox to be identified comprises, but is not limited to, potential financial, cyber and information manipulation and disinformation tools.

## Main Findings

This study delves into the issue of external interference in European elections, highlighting the persistent attempts by malign foreign state and non-state actors to manipulate electoral processes. These interference efforts are driven by the allure of relatively low-cost, high-impact methods that aim to create doubt, suspicion, instability, and division within societies. With numerous cases demonstrating these interference attempts, it is unrealistic to expect the upcoming 2024 European elections to be immune. While acknowledging the persistent threats, it's essential to recognize that there are safeguards in place to counter external interference in European elections, including enhanced information campaigns, election monitoring, and collaborative efforts with tech companies to detect and mitigate disinformation and cyberattacks.

The European Parliament election, consisting of 27 individual elections across the continent, is particularly susceptible to external interference due to its complexity and the potential for a single successful attack in one country to cast doubt on the entire process. Early indicators like DDoS attacks and social engineering tactics suggest the attractiveness of the European elections as targets for malign foreign actors. The ongoing support for Ukraine by EU and NATO countries further raises Europe's profile as a focal point for electoral interventions.

Methods used by foreign malign actors to intervene in elections include financial avenues such as the funding of political parties, politicians, and campaigns, as well as engaging in vote buying, incentivising voters, and leveraging diasporas on behalf of third countries. These direct approaches may be accompanied by orchestrated information manipulation campaigns, including dissemination of disinformation and employing intimidation tactics against critical voices. Malign foreign actors also target the voting process through 'hack and leak' campaigns, DDoS attacks, or compromising electoral infrastructure. Their strategies evolve over time, as they learn from one another's approaches.

Russia and China stand out as key players in electoral interventions across different dimensions. Russia has a history of sowing discord in Europe's elections, while China's involvement is a more recent development, focusing on presenting its authoritarian government in a positive light. Russia employs disruptive tactics, while China emphasises discourse power and attempts to coerce rather than confound. Although both Russia and China engage in election interventions, the former is still more advanced. Nevertheless, a convergence of factors, including Beijing's interest in undermining the US-EU relationship and its track record of amplifying Russian disinformation, endows China with the capacity to evolve into a noteworthy concern over time.

Attribution is complex, and governments may be hesitant to publicly name culprits of electoral interventions due to political ramifications. Although various legislative measures have been implemented to counter interventions, their efficacy hinges on a collaborative effort encompassing society as a whole. A comprehensive strategy involving transparency, resilience, and societal engagement is vital to safeguard the integrity of European elections.

# 1. INTRODUCTION

Foreign interference in democratic processes has become a growing concern in recent years. Malign foreign state and non-state actors have been reported to engage in sophisticated operations to manipulate public opinion, fabricate and spread disinformation, support selected candidates or political parties before elections in order to promote their goals, and coerce or discourage others from running for public offices. This intricate web of interference activities has unveiled a new dimension of challenges that democracies across the globe must confront in order to preserve the integrity of their electoral systems and ensure sovereign control over their domestic affairs.

As the phenomenon of foreign interference continues to permeate on a global scale, there is an inevitability to its impact on the European Union (EU) and its member states. A series of documented attempts to undermine democratic processes within the EU underline the urgency of the matter. In light of the impending 2024 elections, the report released by the European Parliament's Special Committee on foreign interference in all democratic processes in the European Union, including disinformation (INGE 2), has warned against the potential interference and orchestrated information manipulation that may lie ahead.[1]

Electoral interventions by third countries carry a host of detrimental consequences that can undermine the integrity of democratic processes and compromise the sovereignty of nations. Foreign electoral interventions disrupt the fundamental principle of self-determination, as they seek to impose external interests on a nation's electoral outcomes, eroding the democratic sovereignty of the targeted country. At the same time, the perception that electoral outcomes are influenced by external actors erodes public trust in the democratic process, leading to disillusionment and potentially a reduction in political participation. Consequently, it undermines the credibility of elected representatives. An intervention may result in the election of representatives who prioritise foreign interests over domestic needs, and, in extreme cases, it may create economic dependence on the intervening country, subsequently compromising a nation's ability to formulate policies independently.

This study scrutinises the multifaceted landscape of foreign electoral interference, drawing attention to their past manifestations and potential consequences. Its objective is to present European and national decision-makers with a comprehensive analysis of the tools used by malign foreign actors, drawing upon documented cases of interventions in election processes worldwide with a view to formulate policy responses. While it primarily takes an actor-agnostic approach, it closely examines electoral interventions conducted by actors affiliated with the Russian Federation and the People's Republic of China. In several cases it also sheds light on some activities of other powers, offering additional examples to illustrate the plethora of forms

1 European Parliament, Special Committee on foreign interference in all democratic processes in the European Union, including disinformation (INGE 2), Report on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation (2022/2075(INI)), 15 May 2023, p. 13. Available at https://www.europarl.europa.eu/doceo/document/A-9-2023-0187_EN.html (accessed August 2023).

electoral interventions can take. Finally, the likelihood of the described tactics, techniques and procedures (TTPs) being utilised before and after the European elections in June 2024 is assessed.

In this study, foreign electoral interference is understood as 'intentional covert or overt attempts by state or non-state actors to influence electoral processes or public perceptions in order to advantage or disadvantage election contestants in another sovereign country'.[2] The objectives of electoral interventions need not invariably assume an overtly ambitious trajectory, characterised by endeavours like orchestrating regime overthrows. Rather, the propagation of the polarisation of societies, instigating disorder and the erosion of confidence in democratic mechanisms suffice as attainable aims.[3] Empirical studies, notably those conducted by Tomz and Weeks, attest that even seemingly modest instances of electoral intervention have the capacity to 'divide and demoralise the country'.[4]

Foreign interference in electoral processes is certainly not a novelty. It spreads over centuries, transcends the confines of a singular international actor and has exhibited a pervasive presence across diverse geopolitical contexts. Bubeck and Marinov identified electoral interventions in 52 % of elections and partisan interventions geared towards specific candidates in 33 % of elections spanning from 1945 to 2012, encompassing a comprehensive analysis of electoral processes in over a hundred countries.[5] In short, interventions have undeniably constituted a component intrinsic to electoral landscapes, one which has to be anticipated and countered within democratic processes.

While evidence has become increasingly available for more distant historical periods, it is obvious that the termination of the Cold War did not put an end to electoral interventions. To the contrary, they continue to be performed frequently.[6] This trend can be demonstrated by Russia's intervention into the US presidential election in 2016, which has been well-documented and

2 Mohan, V., Wall, A., 'Foreign Electoral Interference: Past, Present, and Future', *Georgetown Journal of International Affairs*, Vol. 20, 2019, p.110.

3 Rosenberg, M., Singer, D.E., Perlroth, N., '"Chaos Is the Point": Russian Hackers and Trolls Grow Stealthier in 2020', 10 January, 2020. Available at https://www.nytimes.com/2020/01/10/us/politics/russia-hacking-disinformation-election.html (accessed August 2023).

4 Tomz, M., Weeks, J., 'Public Opinion and Foreign Electoral Intervention', *American Political Science Review*, Vol. 114, No. 3, August 2020, pp. 857.

5 Bubeck, J., Marinov, N., *Rules and Allies: Foreign Election Interventions*, Cambridge University Press, Cambridge, 2019, p. 111.

6 In fact, Levin using his dataset claims that 18 % of interventions happened after the end of the Cold War (till 2000). See Levin, D. H., 'Will You Still Love Me Tomorrow? Partisan Electoral Interventions, Foreign Policy Compliance, and Voting in the UN', *International Interactions*, Vol. 47, No. 3, 4 May, 2021, p. 462.

studied.[7] The 2018 US midterm election[8] and the 2020 US presidential election[9] were also reported to have been targeted by malign foreign actors. While the US election cycles, with the US being the dominant power in the international system, may have 'naturally' attracted attention, Europe has not been exempted from attempts to intervene in its elections. Examples include the alleged intervention into the UK referendum on Brexit,[10] Russia's involvement in the 2016 coup attempt aimed at preventing Montenegro from joining NATO,[11] the 2018 Macedonian referendum,[12] as well as the 2017 presidential election in France,[13] the German general election in the same year[14] and others.[15]

Moreover, electoral interventions by malign foreign actors, exemplified by Russian and Chinese state and non-state entities, have expanded their geographical scope. Russia reasserted its presence in regions relinquished shortly after the end of the Cold War – a reality exemplified by

7 See United States Senate, 'Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 US Election', Volume 1: Russian Efforts Against Election Infrastructure with Additional Views', 10 November, 2020. Available at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf (accessed August 2023).

8 Dwoskin, E., Romm, T., 'Facebook Says It Shut down 32 False Pages and Profiles Engaged in Divisive Messaging Ahead of the US Midterm Elections', Washington Post, 31 July, 2018. Available at https://www.washingtonpost.com/technology/2018/07/31/facebook-says-it-has-uncovered-coordinated-disinformation-operation-ahead-midterm-elections/ (accessed August 2023).

9 National Intelligence Council, 'Foreign Threats to the 2020 US Federal Elections, National Intelligence Council', 10 March, 2021. Available at https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf (accessed August 2023).

10 Intelligence and Security Committee of UK Parliament, 'Russia', 21 July, 2020, pp. 12-14. Available at https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf (accessed August 2023).

11 Conley, H.A., Melino, M., 'Russian Malign Influence in Montenegro: The Weaponization and Exploitation of History, Religion, and Economics', Center for Strategic and International Studies (CSIS), 14 May, 2019. Available at https://www.csis.org/analysis/russian-malign-influence-montenegro-weaponization-and-exploitation-history-religion-and (accessed August 2023).

12 Santora, M., Barnes, J.E., 'In the Balkans, Russia and the West Fight a Disinformation-Age Battle', The New York Times, 16 September, 2018. Available at https://www.nytimes.com/2018/09/16/world/europe/macedonia-referendum-russia-nato.html (accessed August 2023).

13 Sonne, P., 'A Russian Bank Gave Marine Le Pen's Party a Loan. Then Weird Things Began Happening', Washington Post, 29 December, 2018. Available at https://www.washingtonpost.com/world/national-security/a-russian-bank-gave-marine-le-pens-party-a-loan-then-weird-things-began-happening/2018/12/27/960c7906-d320-11e8-a275-81c671a50422_story.html (accessed August 2023).

14 BBC News, 'Turkey's Erdogan Says German Leaders Are Enemies', 18 August, 2017. Available at https://www.bbc.com/news/world-europe-40973197 (accessed August 2023).

15 For a list of cyber-infused election interventions targeting the European continent see O'Connor, S., Hanson, F., Currey, E., and Beattie, T., *Cyber-Enabled Foreign Interference in Elections and Referendums*, The Australian Strategic Policy Institute, October 2020, pp. 31-45. Available at https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums (accessed August 2023).

its renewed engagement in elections on the African continent.[16] China has ventured into territories hitherto unexplored, as evidenced by its emergent foray into electoral interventions within, for instance, Canada.[17]

All these trends have been reinforced by the digitalisation of elections, the proliferation of social media networks, and the popularity of online communication channels which have exponentially expanded the avenues through which malign foreign actors can infiltrate and manipulate public opinion and electoral processes. The inherent vulnerabilities within these digital landscapes, such as the rapid dissemination of information, the blurring of authentic sources, and the ease of fabricating content aimed at harming political parties or candidates, present an enticing terrain for interveners to exploit. Furthermore, the interconnectedness fostered by online communication has amplified the ripple effects of interventions, enabling their resonance across communities and borders with unprecedented speed and efficacy.

Simultaneously, the utilisation of the digital landscape provides interveners with a conduit for plausible deniability, owing to the inherent difficulty and complexity of attribution, as exemplified by the case of the Brexit referendum. Even in instances where an intervention fails to yield the desired electoral outcome,[18] it can still compel the targeted state to respond, manifesting as the exposure of the intervention attempt, public condemnation, or even countermeasures, such as sanctions against implicated entities. This imperative for responsive action demands a substantial allocation of the targeted state's financial and human resources.

Consequently, electoral interventions emerge as a low-cost, potentially high-gain form of interference, as their repercussions do not elicit the more robust or direct responses to intervention, such as military. At the same time, the capacity of electoral interventions to accentuate polarisation and erode trust in democratic processes within the recipient nations is significant. For these reasons, it is foreseeable that electoral interventions will persist as a prominent instrument within the arsenal of malign foreign state and non-state actors.

A note regarding the rationale behind focusing on Russia and China, though not limiting the study to only these two powers, is warranted at this point. In broad terms, countries engage in election interventions with the aim of cultivating an environment conducive to promoting their strategic, political, and economic objectives. Russia, in particular, holds the belief that election

16 See a useful list of Russia's electoral interventions in Africa in Akinlolu, A., Ogunnubi, O., 'Russo-African Relations and Electoral Democracy: Assessing the Implications of Russia's Renewed Interest for Africa', *African Security Review*, Vol. 30, No. 3, July 3, 2021, p. 387.

17 See Jung, C., 'China's Interference in Canada's Election', The Diplomat, 22 November, 2022. Available at https://thediplomat.com/2022/11/chinas-interference-in-canadas-elections/ (accessed August 2023).

18 These outcomes may be, in fact, quite common. Levin writes that there were 64 successful partisan electoral interventions and 53 unsuccessful interventions from 1946 to 2000. Of these successes 24 (38 %) were overt and the remainder were covert. The US succeeded in 52 of its electoral interventions and failed in 29 of them. The Soviet Union/Russia succeeded in 12 of its electoral interventions and failed in 24. See Levin, D. H., 'Will You Still Love Me Tomorrow? Partisan Electoral Interventions, Foreign Policy Compliance, and Voting in the UN', *International Interactions*, Vol. 47, No. 3, 4 May, 2021, p. 457.

interference is merely a pursuit undertaken by all governments to further their interests.[19] However, it's important to note that both Russia and China are governed by leaders who perceive their countries to be enmeshed in an information conflict with western counterparts.[20] 'Sowing chaos' and divisions within western societies,[21] undermining the credibility of western democracy[22] by eroding the democratic institutions, processes and civil society organisations,[23] 'challenging the western democratic system in the eyes of transitioning democracies' and 'undermining the transatlantic alliance and the European project'[24] are all perceived as a proportional response to the alleged interference by western nations, particularly the United States, in the domestic affairs of Russia and China.[25]

The Australian Strategic Policy Institute (ASPI) report on cyber-enabled election interventions asserts that 'many of Russia's efforts remain focused on Europe.' According to the report, Russia intervened in 20 European elections, including the 2019 European Parliament election and seven referendums.[26] Given the historical backdrop replete with instances of electoral interventions by the USSR/Russia in Europe, coupled with the EU's enforcement of sanctions as a response to Russia's invasion of Ukraine, the potential for further interventions within the EU's democratic framework from Russia is palpable.

---

19 Sherman, J., 'Changing the Kremlin's Election Interference Calculus', *The Washington Quarterly*, Vol. 45, No. 1, 2 January, 2022, p. 120.

20 Galeotti, M., 'Active Measures: Russia's Covert Geopolitical Operations', George C. Marshall European Center For Security Studies, June 2019. Available at https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0 (accessed August 2023); Charon, P., Jeangène Vilmer, J.B., *Chinese Influence Operations*, Report by the Institute for Strategic Research (IRSEM), Paris, Ministry for the Armed Forces, October 2021. Available at https://www.irsem.fr/report.html (accessed August 2023).

21 Marks, J., 'Is Russia or China the Biggest Cyber Threat? Experts Are Split', Washington Post, 20 January, 2022. Available at https://www.washingtonpost.com/politics/2022/01/20/is-russia-or-china-biggest-cyber-threat-experts-are-split/ (accessed August 2023).

22 Dorell, O., 'Alleged Russian Political Meddling Documented in 27 Countries since 2004', USA TODAY, 7 September, 2017. Available at https://www.usatoday.com/story/news/world/2017/09/07/alleged-russian-political-meddling-documented-27-countries-since-2004/619056001/ (accessed August 2023).

23 Barros, B., Soula. E., 'Here and Now: Chinese Interference in the Transatlantic Space', Alliance For Securing Democracy - German Marshall Fund, 9 February, 2021. Available at https://securingdemocracy.gmfus.org/here-and-now-chinese-interference-in-the-transatlantic-space/ (accessed August 2023).

24 Lamond, J., Dessel, T., 'Democratic Resilience A Comparative Review of Russian Interference in Democratic Elections and Lessons Learned for Securing Future Elections', Center for American Progress, September 2019. Available at https://www.americanprogress.org/article/democratic-resilience/ (accessed August 2023).

25 Korsunskaya, D., 'Putin Says Russia Must Prevent "Color Revolution"', Reuters, 20 November, 2014. Available at https://www.reuters.com/article/us-russia-putin-security-idUSKCN0J41J620141120 (accessed August 2023); Global Times, 'US' NED "Mastermind" behind Global Separatist Riots, Color Revolutions, Political Crises: Chinese FM Report', 8 May, 2022. Available at https://www.globaltimes.cn/page/202205/1265027.shtml (accessed August 2023).

26 O'Connor, S., Hanson, F., Currey, E., and Beattie, T., *Cyber-Enabled Foreign Interference in Elections and Referendums*, The Australian Strategic Policy Institute, October 2020, p.13. Available at https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums (accessed August 2023).

Likewise, China seems to hold similar views towards dangers posed to its regime by the West.[27] Yet in the domain of election interventions, in comparison to Russia, China is a relative latecomer. Regarding cyber-enabled interventions, experts agree that while Russia presents a more imminent threat than other state actors, it is China who is more threatening in the long run.[28] This is due to the fact that Beijing's cyber activities are driven by different motivations than Russia's. While Russia seeks to 'only' sow discord, China wants to 'reshape the international system conforming to its ideology'[29] and 'elevate its authoritarian approach as superior to western democracy'.[30]

It is again in the realm of information manipulation, where China's interference within European contexts, manifestly inspired by Russia's tactics, is prominently evidenced as illustrated by the dissemination of COVID-19 origin-related disinformation[31] across Europe as well as the circulation of Russia's standpoint[32] regarding the causes of war in Ukraine. Moreover, China has displayed increasing adeptness in harnessing algorithms and orchestrating social media campaigns, as exemplified by its involvement in the 2000 Taiwan elections. In a significant development, Twitter (now X) disclosed in October 2022 that it had discontinued multiple China-linked accounts which posted inflammatory content about the 2020 US elections, including false claims of election rigging and right-wing extremist content which alluded to the QAnon conspiracy theory.[33]

27 Leonard, M., Bachulska, A., 'China and Ukraine: The Chinese Debate about Russia's War', Policy Brief, European Council on Foreign Relations, July 11, 2023. Available at https://ecfr.eu/publication/china-and-ukraine-the-chinese-debate-about-russias-war-and-its-meaning-for-the-world/ (accessed August 2023).

28 Marks, J., 'Is Russia or China the Biggest Cyber Threat? Experts Are Split', Washington Post, 20 January, 2022. Available at https://www.washingtonpost.com/politics/2022/01/20/is-russia-or-china-biggest-cyber-threat-experts-are-split/ (accessed August 2023).

29 Marks, J., 'Is Russia or China the Biggest Cyber Threat? Experts Are Split', Washington Post, 20 January, 2022. Available at https://www.washingtonpost.com/politics/2022/01/20/is-russia-or-china-biggest-cyber-threat-experts-are-split/ (accessed August 2023).

30 Watts, C., 'Who Cares about a Midterm Election? Comparing Russia, Iran, and China's Electoral Interference from Past to Present', Alliance For Securing Democracy - German Marshall Fund, 19 May, 2022. Available at https://securingdemocracy.gmfus.org/who-cares-about-a-midterm-election-comparing-russia-iran-and-chinas-electoral-interference-from-past-to-present/ (accessed August 2023).

31 Rankin, J., 'EU Says China behind 'huge Wave' of Covid-19 Disinformation', The Guardian, 10 June, 2020. Available at https://www.theguardian.com/world/2020/jun/10/eu-says-china-behind-huge-wave-covid-19-disinformation-campaign (accessed August 2023).

32 Karásková, I., et al., *Backing Russia on Ukraine: China's Messaging in Central and Eastern Europe*, Association for International Affairs (AMO), Prague, Czech Republic, May 2022.

33 Collier, K., 'Pro-China Social Media Campaign Sought to Influence US Voters, Researchers Say', NBC News, 26 October, 2022. Available at https://www.nbcnews.com/tech/security/-china-social-media-campaign-sought-influence-us-voters-researchers-sa-rcna53728 (accessed August 2023).

China's (cyber-enabled) electoral interventions have already encompassed no fewer than 10 elections in seven distinct countries, primarily concentrated within the Asia-Pacific region.[34] Since the 1996 Taiwan missile crisis, which was aimed at intimidating the Taiwanese electorate ahead of the presidential elections, China's strategy and tactics in electoral interventions have undergone a noteworthy evolution, reflecting a strategic shift in its objectives and methods. Initially focused on curbing the 'separatism' of Taiwan, China's approach has progressively evolved to encompass the broader goal of undermining the credibility of democratic processes and capitalising on cultural divisions within societies. These goals are similar to Russia's and Iran's. The transition in objectives has been accompanied by a distinct transformation in tactics. While early electoral interventions were characterised by the overt display of hard power, such as missile exercise in the Taiwan Strait in 1996, China has gradually transitioned towards employing more sophisticated and covert methods of interference.[35] This shift underscores China's recognition of the limitations of overt military displays and the efficacy of subtler manoeuvres in achieving its objectives in the realm of electoral influence.

Notably, empirical evidence regarding Chinese election interventions within Europe remains limited in open-source data. Plausible explanations encompass the possibility that China's interest in influencing European election outcomes itself may be limited. Equally possible is that such interventions have occurred but have yet to be unearthed or reported. An alternative hypothesis posits that China's interventions may have occurred but without the requisite magnitude to trigger a response, with counterintelligence agencies remaining vigilant, albeit without public disclosure of pertinent information.[36] However, there is no doubt that China has already demonstrated its capability and resolve to meddle in electoral processes across different global contexts. It is our responsibility to take under careful consideration the possibility that China might decide to intervene in the upcoming 2024 European elections. Ignoring this potential scenario would constitute an act of negligence.

The shared underpinning of electoral interventions resides in the manipulation of people, extending beyond the mere manipulation of the systems people engage with.[37] Authoritarian regimes present to the world a story portraying Western democracies as flawed and corrupt. By doing so, they erode trust in democratic processes in the targeted countries and, at the same time, increase the likelihood that their own population will not seek change. A remedy lies in

34 O'Connor, S., Hanson, F., Currey, E., and Beattie, T., *Cyber-Enabled Foreign Interference in Elections and Referendums*, The Australian Strategic Policy Institute, October 2020, pp. 31-45. Available at https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums (accessed August 2023).

35 Wilson, K.L., 'Strategic Responses to Chinese Election Interference in Taiwan's Presidential Elections', *Asian Perspective*, Vol. 46, No. 2, March 2022, pp. 255–277.

36 For the discussion on lack of information on electoral interventions shared by counterintelligence agencies with the public, see Chapter 2.2.

37 Clough, A., de Avila, A., 'In Guarding Democracy, Hindsight Really Will Be 2020: The Tabletop Exercise as a Model for Securing American Elections', *Kennedy School Review*, Volume XX, 15 October, 2020. Available at https://ksr.hkspublications.org/2020/10/15/in-guarding-democracy-hindsight-really-will-be-2020-the-tabletop-exercise-as-a-model-for-securing-american-elections/ (accessed August 2023).

increasing the transparency and resilience of the electoral processes in democracies, and, simultaneously, increasing the costs for interveners. This study aims to help by raising awareness about how malign foreign state and non-state actors might intervene in European elections. This way, both decision-makers and the public can be better prepared. As the saying goes, sunlight is often the most effective disinfectant.

# 2. HOW MALIGN FOREIGN ACTORS INFLUENCE ELECTIONS

The following chapter focuses on three types of potential election interventions that the authors believe could occur on the eve of the 2024 European elections – (1) financial incentives provided by malign foreign state and non-state actors, (2) information manipulation and (3) cyber-enabled interference in elections. While, for the sake of clarity, the study treats these types of election interventions as separate, in reality they often are interlinked. For instance, spear phishing may provide an intervener with sensitive information which may then be used in operations aimed at harming a political candidate, while the malign foreign actor provides financial and media support to the rival contestant.

In this context, it's noteworthy that instances of electoral intervention seldom transpire without the awareness and active collaboration of the political candidate involved.[38] Furthermore, such interventions commonly entail a reciprocal arrangement, wherein the candidate commits to certain policies in return for the intervener's assistance in securing or maintaining their position.[39] The transactional nature of partisan electoral intervention implies that it can lead not only to the emergence of a political representative aligned with the intervener's interests but also potentially yield lasting repercussions on the policies of the targeted nation.

Thus, from among the three domains explored within the purview of this study – namely, financial instruments, information manipulation, and cyberattacks – it is the allure of financial incentives that the authors identify as the most concerning and unsettling. Information manipulation, while capable of bolstering a candidate's electoral prospects, assumes a more pivotal role in fostering heightened social tensions and sowing the seeds of public mistrust. In contrast, the prospect of altering an election's outcome solely through cyber operations remains improbable.

Similarly, it's not necessarily a given that the candidate benefiting from these actions would be knowledgeable about information manipulation and cyberattacks. The very nature of these tactics allows for a level of deniability. On the other hand, it may be more difficult (though not impossible, as the following sub-chapter demonstrates) to conceal the acceptance of financial incentives by a candidate or a party.

## 2.1. Financial interference

### 2.1.1. Background

Through the provision of financial support to a candidate or political party, malign foreign actors wield the capacity to exert influence and advance specific policy agendas. They may retain a significant leverage over candidates well beyond election. Thus, the provision of financial

[38] Levin, D. H., *Meddling in the Ballot Box: The Causes and Effects of Partisan Electoral Interventions*, 1st ed., Oxford University Press, 2020.

[39] Levin, D. H., 'Will You Still Love Me Tomorrow? Partisan Electoral Interventions, Foreign Policy Compliance, and Voting in the UN', *International Interactions*, Vol. 47, No. 3, May 4, 2021, p. 454.

incentives to political parties and candidates by third countries raises significant ethical and political concerns.

Accepting financial support from third countries can lead to an erosion of a country's ability to set its own policies, create a dependency on foreign donors, fuel corruption, and potentially lead to compromised decision-making. Considering the high costs tied to running election campaigns, providing financial support can give a supported candidate a substantial advantage. This assistance can upset the balance that domestic campaign finance laws – which regulate and sometimes limit the kinds and amounts of financial support candidates receive – aim to establish.[40] As a result, the foreign financial incentives distort the level playing field in the electoral process.

While significant attention has been paid to political parties or representatives at the national level, less attention has been devoted so far to regional and local levels, where an understanding of the pitfalls associated with financial offers made by third country actors remains limited. Notably, China's strategic overtures for political influence frequently target officials at the provincial and municipal levels, [41] a factor that accentuates the significance of these under-regulated strata in the context of electoral interventions and the need to approach the issue of countering election interventions via financial means in a holistic way.

An intervener's strategic focus on provincial or municipal tiers of governance can be fortified through the adroit utilisation of ethnic diasporas. While the tactical deployment of this approach by Russia appears to be relatively subdued, possibly attributed to potential electoral reservations pertaining to regions such as Central and Eastern Europe, where Russian descent might not be greeted favourably by the electorate, China has exhibited an inclination to actively leverage its own ethnic and diasporic enclaves. Reports have emerged documenting China's engagement in incentivising Chinese communities abroad to champion politicians who espouse pro-China stances, orchestrating multifaceted campaigns spanning both offline and online domains to bolster selected candidates, and, in some instances, resorting to influencing electoral outcomes through the acquisition of votes (see Chapter 2.1.2). This calculated manoeuvring underscores China's adeptness at exploiting its diaspora as a potent instrument for shaping foreign political landscapes in alignment with its strategic interests.

Lastly, a linked concern pertains to the utilisation of geoeconomics by third countries, which can either advance or hinder the prospects of a preferred political candidate or party. This situation encompasses scenarios where offers to establish trade relationships, facilitate transport and communication channels,[42] provide advantages to the candidate's electoral support base, or

40 Reimann, N., 'Foreign Electoral Interference Normative Implications in Light of International Law, Human Rights, and Democratic Theory', Dissertation, University of Zurich, 2023, p. 29. Available at https://www.zora.uzh.ch/id/eprint/233343/ (accessed August 2023).

41 Alliance Canada Hong Kong, 'In Plain Sight: Beijing's Unrestricted Network of Foreign Influence in Canada', May 2021. Available at https://alliancecanadahk.com/wp-content/uploads/2022/06/ACHK_InPlainSight.pdf (accessed August 2023).

42 Wilson, K.L., 'Strategic Responses to Chinese Election Interference in Taiwan's Presidential Elections', *Asian Perspective*, Vol. 46, No. 2, March 2022, pp. 255–277.

conversely, issue threats of disinvestment[43] from the country, come into play. This tactical dimension is exemplified in instances like Russia's utilisation of gas in relations with Europe or China's policies of aligning economic interests with political influence through the Belt and Road Initiative (BRI). China has been willing to utilise geoeconomics as exemplified by its imposition of sanctions affecting trade with Australia,[44] following Australia's calls for an independent investigation into the origins of COVID-19, or the imposition of trade barriers against Lithuania[45] due to the establishment of the Taiwanese Representative Office in Vilnius. The underlying rationale guiding the implementation of these robust economic measures such as trade sanctions and the establishment of trade barriers, is to impose repercussions on an entire country for the actions of its political representatives which China perceives as unfavourable.

A distinct and notable scenario arises when companies operating within the intervener's market become the focal point. In this case, the intervener may strategically 'outsource' pressure on political representatives to be executed by other entities. Such tactics are based on an assumption that the impacted entrepreneurs, motivated by safeguarding their business interests, will exercise influence over their own domestic political representation to prevent adverse repercussions on their enterprises.[46] In these cases, the targeted entity is not a candidate or party but an enterprise with which a candidate or party is involved, or financially dependent on.

### 2.1.2. Methods

This sub-section delves into the realm of financial mechanisms employed for electoral interventions. While the purview of this concept may be extensive, this study purposefully hones in on a specific dimension: the financing of political parties, candidates and campaigns, incentives provided to an electorate, utilisation of diasporic communities, and the practice of vote buying. Other plausible avenues of influence, such as the sponsorship of cultural and religious endeavours, or rendering aid, are intentionally omitted from this study. While these

43 Karásková, I., et al., *China's Sticks and Carrots in Central Europe: The Logic and Power of Chinese Influence*, Association for International Affairs (AMO), 2020.

44 Armstrong, S., 'Learning the Right Lessons from Chinese Sanctions on Australian Imports', East Asia Forum, 16 April, 2023. Available at https://www.eastasiaforum.org/2023/04/16/learning-the-right-lessons-from-chinese-sanctions-on-australian-imports/ (accessed August 2023).

45 Janeliūnas, T., Boruta, R., 'Lithuania's Confrontation with China Over Taiwan: Lessons from a Small Country', Global Taiwan Institute, 27 July, 2022. Available at https://globaltaiwan.org/2022/07/lithuanias-confrontation-with-china-over-taiwan-lessons-from-a-small-country/ (accessed August 2023).

46 The subject under consideration is frequently brought up in discussions regarding German companies operating within the Chinese market. However, it's essential to note that similar instances have arisen, such as the perceived potential harm to Czech companies in China due to the visit to Taiwan by the Czech Senate President. This strategic approach was built upon the assumption that businesses with vested interests in the Chinese market would take measures to ensure that the Czech politician refrained from taking any actions that could be interpreted as provocative towards China. For more insights into this topic, see Karásková, I., et al., *China's Sticks and Carrots in Central Europe: The Logic and Power of Chinese Influence*, Association for International Affairs (AMO), 2020. For a detailed analysis of how Taiwanese businesses in China are leveraged during Taiwan elections, see Wilson, K.L., 'Strategic Responses to Chinese Election Interference in Taiwan's Presidential Elections', *Asian Perspective*, Vol. 46, No. 2, March 2022, pp. 255–277.

aforementioned avenues have undoubtedly been pursued to support particular candidates in the past, their comprehensive consideration would dilute the study's focal objective. This objective is to pinpoint the most salient and concerning facets of election interventions that are likely to manifest within European electoral contexts.

- **Financing political parties and candidates**

Election interventions via financial means are often facilitated through mechanisms such as direct donations, loans, or other financially advantageous transactions conducted at both central as well as local government levels. The issue is far from academic, as well-documented examples from the European context show. Russia, for instance, extended significant financial means to notable political recipients, including the National Front in France,[47] the Five Star Movement in Italy, and the Syriza Party in Greece.[48]

The European Union acknowledges the challenges posed by donations from third countries to political parties and candidates. Regulation (EU, Euratom) 1141/2014[49] prohibits European political parties and foundations from accepting donations or contributions that lack transparency, including anonymous sources. Similarly, the regulation extends its purview to preclude the acceptance of financial support from public authorities either within Member States or third nations, as well as from enterprises subject to the direct or indirect sway of such public entities, owing to ownership, financial engagement, or governing principles. Correspondingly, the regulation also mandates the exclusion of contributions from private entities domiciled in third countries, as well as from individuals not endowed with the right to partake in European Parliament elections.

Nonetheless, at the national level within several EU member states, a comprehensive prohibition of third-country donations has not been uniformly enacted. While all EU member states have adopted regulations regarding the reporting and public disclosure of donations, conditions for reporting and disclosure vary.[50] Moreover, donations to political parties may come not just in a monetary form, but rather contributions in-kind, such as buying media space for promotion of a

47 National Assembly of the French Republic, 'Rapport fait au nom de la commission d'enquête, relative aux ingérences politiques, économiques et financières de puissances étrangères – États, organisations, entreprises, groupes d'intérêts, personnes privées – visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques français', 1 June, 2023. Available at https://www.assemblee-nationale.fr/dyn/16/rapports/ceingeren/l16b1311-t1_rapport-enquete (accessed August 2023).

48 Noack, R., 'Everything We Know So Far about Russian Election Meddling in Europe', Washington Post, 10 January, 2018. Available at https://www.washingtonpost.com/news/worldviews/wp/2018/01/10/everything-we-know-so-far-about-russian-election-meddling-in-europe/ (accessed August 2023).

49 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 ('Regulation 1141/2014'). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R1141 (accessed August 2023).

50 European Commission, Directorate-General for Internal Policies of the Union, Reed, Q., Jouan Stonestreet, B., Devrim, D. et al., *Financing of political structures in EU Member States – How funding is provided to national political parties, their foundations and parliamentary political groups, and how the use of funds is controlled*, European Parliament, 2021. Available at https://data.europa.eu/doi/10.2861/932651 (accessed August 2023).

selected candidate or a party.[51] This conduct, while not illegal, can still distort the election environment.

While a majority of EU member states have full or partial bans on foreign donations to political parties and candidates, political figures may find loopholes and creative ways of circumventing the regulations.[52] A case in point may be the allegations that a national political party in Italy had sought millions of euro from Russian investors via a secret oil deal.[53] According to the allegations, an associate of that party's leader met with unidentified Russians in Moscow's Metropol hotel and discussed a deal in which Russia would sell 3 million tonnes of diesel to an Italian company Eni, from which the money could be diverted.

Similarly, while France bans foreign donations to political parties, the regulation does not prohibit loans. In 2014, a national political party in France obtained a loan of EUR 9 million from the Moscow-based First Czech Russian Bank. The acquisition of the loan coincided with Russia's annexation of Crimea and there were accusations that the stances presented by the National Front on Crimea echoed Russian talking points.[54] Emmanuel Macron cited the loan in his campaign, accusing Marine Le Pen of siding with Russia, when he said: 'When you speak to Russia, you are not speaking to any foreign leader, you are talking to your banker.'[55]

In Germany, which has strict rules on the funding of political campaigns from outside of the EU, the media caused a stir by reporting that three members of one national political party flew to Moscow on a jet provided by a donor during the 2017 campaign.[56]

Russia has gained unequivocal notoriety for its extensive utilisation of financial instruments and in-kind contributions offered by actors with links to the state to bolster political parties or individual candidates on a global scale. This strategic approach has caught the attention of the international community. A notable disclosure came from the US State Department, which

51 Schmitt, G., Mazza, M., *Blinding the Enemy: CCP Interference in Taiwan's Democracy*, Global Taiwan Institute, October 2019. Available at https://globaltaiwan.org/wp-content/uploads/2022/08/GTI-CCP-Interference-Taiwan-Democracy-Oct-2019-final.pdf (accessed August 2023).

52 Soula, E., 'The Many Faces of Foreign Interference in European Elections', German Marshall Fund of the United States. Available at https://www.gmfus.org/news/many-faces-foreign-interference-european-elections (accessed August 2023).

53 Dos Santos, N., 'Investigation into Matteo Salvini's Lega Party's Possible Scheme with Russia', CNN, 11 July, 2019. Available at https://edition.cnn.com/2019/07/11/europe/investigation-league-salvini-russia-money-intl/index.html (accessed August 2023).

54 Salvi, E., Suc, M., Turchi, M., 'Un rapport parlementaire révèle dix ans de connivence entre la Russie et le RN', Mediapart, 1 June, 2023. Available at https://www.mediapart.fr/journal/politique/010623/un-rapport-parlementaire-revele-dix-ans-de-connivence-entre-la-russie-et-le-rn (accessed August 2023).

55 Dodman, B., 'Le Pen's Far Right Served as Mouthpiece for the Kremlin, Says French Parliamentary Report', France 24, 3 June, 2023. Available at https://www.france24.com/en/france/20230603-le-pen-s-far-right-served-as-mouthpiece-for-the-kremlin-says-french-parliamentary-report (accessed August 2023).

56 Deutsche Welle, 'Report: Russian Money Fueled AfD Trip', 22 May, 2018. Available at https://www.dw.com/en/report-afd-members-flight-sponsored-with-russian-money/a-43872774 (accessed August 2023).

highlighted findings from the 2022 US Intelligence Review. This report revealed that Russia had clandestinely channelled a sum of at least USD 300 million towards political parties, government officials, and politicians across over two dozen countries, commencing from 2014.[57]

While Russia's use of financial tools has garnered much of the international attention, it is crucial to acknowledge that China has also been steadily intensifying its engagement in this arena, mostly in the countries of Asia-Pacific. Notably, China's interventions hold a significant foothold in Taiwan, where China capitalises on linguistic and cultural similarities. This positions Taiwan as a recurrent target for Chinese interventions and enables the study of China's adept utilisation of economic leverage through a nuanced framework of rewards and punishments offered to both the Taiwanese electorate and political parties. By deftly applying this 'carrots and sticks' paradigm, China restricts benefits to candidates perceived as independence-leaning, while favouring those aligned with its interests.[58]

The cases of China's funding around Taiwanese political parties offer a glimpse of China's tactics, though it does not follow that the same pattern is used elsewhere. In 2019, Taiwanese retired military officer Luo Wen-shan was sentenced to two years and six months in prison for accepting nearly TWD 10 million in political contributions and donations to be used to buy media ads on behalf of an organisation Luo chaired and in support of Kuomintang (KMT) presidential candidate Ma Ying-jeou.[59] This shows how domestic organisations may be utilised to obscure the source of funding and empower preferred candidates during campaigns.

Australia encountered a noteworthy episode in 2019, described as a perceived endeavour to infiltrate the nation's parliament. This case, featuring Liberal party member Nick Zhao, reportedly involved an offer of AUD 1 million from Chinese operatives with the aim of influencing electoral outcomes.[60] Nick Zhao was discovered dead in a hotel room shortly before a scheduled court appearance, where he purportedly intended to disclose information about the fraudulent offer and the associated financial arrangements.[61]

Allegations of potential Chinese electoral interventions have reverberated within the political landscape of Canada as well. This particular instance echoes the recurring theme of limited transparency, stemming from authorities' reluctance to divulge intelligence due to its sensitive

57 Wong, E., 'Russia Secretly Gave $300 Million to Political Parties and Officials Worldwide, US Says', The New York Times, 13 September, 2022. Available at https://www.nytimes.com/2022/09/13/us/politics/russia-election-interference.html (accessed August 2023).

58 Wilson, K.L., 'Strategic Responses to Chinese Election Interference in Taiwan's Presidential Elections', *Asian Perspective*, Vol. 46, No. 2, March 2022, pp. 255–277.

59 Lin, C., '退將羅文山涉收政治獻金 金主是中共全國政協委員', 中央社 CNA, 3 December, 2019. Available at https://www.cna.com.tw/news/firstnews/201912030181.aspx (accessed August 2023).

60 Lavalette, T., 'Australia Investigates China Plot to Plant Spy in Parliament', AP News, 25 November, 2019. Available at https://apnews.com/article/f60823ab8cc74803bb687d25c54824bf (accessed August 2023).

61 The death sparked conspiracy theories, however, the coroner report assessed Nick Zhao committed suicide. Sakkal, P., McKenzie, N., 'Death of Melbourne-Based Chinese Spy Target "not Suspicious" Says Coroner', The Age, 21 September, 2020. Available at https://www.theage.com.au/national/victoria/death-of-melbourne-based-fraudster-not-suspicious-says-coroner-20200921-p55xmd.html (accessed August 2023).

nature. The core of these allegations emerges from leaked intelligence reports, which assert that Chinese diplomats and their proxies situated within Canada attempted to manipulate election outcomes. Reportedly, the Chinese government employed covert channels to extend secret funding through its Toronto consulate to a cohort of 11 candidates who contested the 2019 federal election. This included discreet financial transfers made 'through intermediaries to candidates affiliated with the Chinese Communist Party (CCP), placing agents into the offices of MPs in order to influence policy, seeking to co-opt and corrupt former Canadian officials to gain leverage in Ottawa, and mounting aggressive campaigns to punish Canadian politicians whom the People's Republic of China (PRC) views as threats to its interests'.[62]

- **Financing political campaigns**

Comprehensive revelations concerning financial transactions directed towards financing political campaigns in Europe from third countries are rare. A notable exception, shedding some light on Russia's tactics, is a 2023 report published by the National Assembly. According to the report, 'François Bayrou confirmed in 2004 that Russian nationals had offered to "pay all of his campaign expenses" during the 2002 presidential election.' Also, in 2016, an adviser to Jean-Luc Mélenchon was 'offered EUR 500 000 in cash for the latter's campaign' by an officer of the GRU, the Russian military intelligence service.[63]

Indeed, a notable trend observed in numerous analytical reports is the avoidance of overtly alleging direct financial entanglements between political parties in Europe and malign foreign actors. This restrained stance can be attributed, in part, to the reluctance of authorities to divulge sensitive information that underpins such allegations. Moreover, the intricacies of detecting and attributing responsibility to the culprits present significant challenges, further complicating the ability to definitively pinpoint instances of foreign financial influence on domestic political processes. When it comes to Russia's support of the European far right, Ramos and Raab observe: 'It is suspected that Russia is quite involved with the campaigns, but is clever about skirting the strict party-funding laws, such as using in-country contacts or bank transfers in Switzerland.'[64]

Indeed, the contact is often made via an intermediary. One such example was an offer of USD 500 billion made to the Catalonian government to aid their attempts to make the region an independent state in 2017 by a former Russian diplomat Nikolai Sadovnikov, whom Catalonian independence leaders described as 'Putin's envoy'.[65] In this specific case, a suspicious component

62 Cooper, S., 'Canadian Intelligence Warned PM Trudeau That China Covertly Funded 2019 Election Candidates: Sources', Global News, 7 November, 2022. Available at https://globalnews.ca/news/9253386/canadian-intelligence-warned-pm-trudeau-that-china-covertly-funded-2019-election-candidates-sources/ (accessed August 2023).

63 National Assembly of the French Republic, 'Rapport fait au nom de la commission d'enquête, relative aux ingérences politiques, économiques et financières de puissances étrangères – États, organisations, entreprises, groupes d'intérêts, personnes privées – visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques français', 1 June, 2023. Available at https://www.assemblee-nationale.fr/dyn/16/rapports/ceingeren/l16b1311-t1_rapport-enquete (accessed August 2023).

64 Ramos, J. M., and Raab, N., 'Russia Abroad, Russia at Home: The Paradox of Russia's Support for the Far Right', *Russian Politics*, Vol. 7, No. 1, March 8, 2022, pp. 80-81.

65 Baquero, A., Hall, K.G., Tsogoeva, A., Albalat, J. G., Grozev, C., Bagnoli, L., Vergine, S., 'Fueling Secession, Promising Bitcoins: How a Russian Operator Urged Catalonian Leaders to Break With Madrid', Organized Crime and Corruption

(a request to make Catalonia a crypto currency haven) may have been included to obfuscate ties to a foreign government.

In regards to China, there are indications that Chinese diplomats and intermediaries in Canada facilitated undisclosed monetary contributions to political campaigns, supplemented by the enlistment of international Chinese students to volunteer full-time for select candidates. The aim of these efforts was to ensure the re-election of the Liberal Party of Canada in 2021. This objective was pursued not with the intent of achieving a majority government, but rather with the aim of establishing a minority government scenario.[66]

### Box 1: Exchanging financial contributions for shifts in stance on South China Sea

Country(ies) affected: Australia

What happened: The New South Wales Labor Party Senator Sam Dastyari resigned following revelations that his vocal alignment with China's stance on the South China Sea coincided with a substantial donation from Chinese billionaire property developer Huang Xiangmo during a 2016 election campaign. Subsequent revelations unveiled the precarious nature of this financial nexus, as Huang reportedly exerted pressure by threatening to withdraw financial support to the Labor Party unless it altered its position on the South China Sea. Moreover, it turned out that Huang had previously paid Dastyari's legal bills.

How it was detected: The case was first reported by a Sydney-based Chinese-language newspaper in 2016. Dastyari denied the allegations, however, later a tape recording of the press conference confirming the claims emerged via Fairfax Media.

Why it matters: The intertwining of donations and political positions points to the ethical dimensions of contributions with implicit expectations.

Source: McKenzie, N., Massola, J., Baker, R., '"It Isn't Our Place": New Tape of pro-Beijing Comments Puts More Heat on Dastyari', The Sydney Morning Herald, 29 November, 2017. Available at https://www.smh.com.au/politics/federal/it-isnt-our-place-new-tape-of-probeijing-comments-puts-more-heat-on-dastyari-20171128-gzuiup.html (accessed August 2023); Hartcher, P., 'Sam Dastyari: Riding the Red Dragon Express Not a Good Look', The Sydney Morning Herald, 3 September, 2016. Available at https://www.smh.com.au/opinion/sam-dastyari-riding-the-red-dragon-express-not-a-good-look-20160902-gr7tcy.html (accessed August 2023); Massola, J., 'Chinese Donor the Yuhu Group Steps in to Help Sam Dastyari', The Sydney Morning Herald, 27 March, 2015. Available at https://www.smh.com.au/politics/federal/chinese-donor-the-yuhu-group-steps-in-to-help-sam-dastyari-20150327-1m9be2.html (accessed August 2023).

Reporting Project, 8 May, 2022. Available at https://www.occrp.org/en/investigations/fueling-secession-promising-bitcoins-how-a-russian-operator-urged-catalonian-leaders-to-break-with-madrid (accessed August 2023).

66 The Globe and Mail, 'CSIS Documents Reveal Chinese Strategy to Influence Canada's 2021 Election', 17 February, 2023. Available at https://www.theglobeandmail.com/politics/article-china-influence-2021-federal-election-csis-documents/ (accessed August 2023).

- **Providing incentives to the electorate**

While the financing of political parties, candidates, and campaigns inherently encompasses a dimension of influencing the electorate, malign foreign actors extend their engagement by directly targeting supporters of specific political factions. An illustrative instance emerges in the context of Taiwan's elections, wherein China orchestrated a multi-faceted approach. Preceding the elections, China offered discounted flights through state-owned carriers from regions in mainland China inhabited by Taiwanese businesspeople back to Taiwan, with an underlying assumption that they would cast their votes in favour of the KMT party. Concurrently, China strategically opened its market to accommodate agricultural products from Taiwan's southern farmers, a core constituency traditionally aligned with the rival Democratic Progressive Party (DPP). This calculated manoeuvre aimed to erode the robust support that the southern farmers typically lend to Taiwan's pro-independence DPP.[67]

Another distinct and targeted strategy involves the utilisation of underground gambling networks within Taiwan. Operating as conduits of influence on behalf of China, these gambling establishments strategically offer favourable odds for a preferred candidate's victory, which incentivises gamblers and their families to actively vote in favour of the endorsed candidate. This intricate manipulation underscores the innovative avenues through which malign foreign actors seek to shape electoral outcomes, leveraging illicit networks as vehicles for orchestrating and channelling support.[68]

Interestingly, should the inducements fail to yield the intended results, China has displayed a willingness to resort to punitive measures. This tactical shift becomes evident in the context of those Taiwanese small and medium enterprises (SMEs) conducting operations within mainland China. Reports have surfaced indicating that China has employed coercive tactics, including the threat of tax inspections and the imposition of fines, as mechanisms to sway businesses into aligning with pro-unification political candidates.[69]

These cases serve as compelling examples that reaffirm the assertion made by the authors regarding the multifarious channels exploited by foreign election interveners. Offering inducements is often matched with punishments in order to bolster specific party or candidates.

- **Targeting diasporic communities**

A note of prudence is essential in evaluating the implications of malign foreign actors engaging with their diasporic communities. The authors emphasize that a mere presence of a diaspora should not be hastily construed as an inherent security concern for democratic countries.

67 Wilson, K.L., 'Strategic Responses to Chinese Election Interference in Taiwan's Presidential Elections', *Asian Perspective*, Vol. 46, No. 2, March 2022, p. 267.

68 Schmitt, G., Mazza, M., *Blinding the Enemy: CCP Interference in Taiwan's Democracy*, Global Taiwan Institute, October 2019. Available at https://globaltaiwan.org/wp-content/uploads/2022/08/GTI-CCP-Interference-Taiwan-Democracy-Oct-2019-final.pdf (accessed August 2023).

69 Qian, L., '中國策動台商資助介選 中南部企業涉入 調局立案蒐證', Liberty Times Net, 24 April, 2023. Available at https://news.ltn.com.tw/news/politics/paper/1579196 (accessed August 2023).

However, it is equally important to study the phenomenon as attempts to (ab)use diaspora constitute a distinctive tactical manoeuvre employed by various malign foreign state actors.

This tactic aims at mobilising support or exerting pressure on political adversaries within democratic countries during electoral periods. It intends to leverage the presence of diasporic communities as a means to either galvanise backing for favoured candidates or apply coercive influence to undermine critical voices within political parties. Malign foreign actors exploit these networks to either bolster candidates who embrace divisive or extremist policies or to provide illicit financial support to parties in nations where such contributions are strictly regulated.

An illustrative case pertains to the actions of Türkiye's President, Recep Tayyip Erdoğan, during the 2017 German elections. In this instance, Erdoğan publicly urged Turkish citizens to cast their votes against three major parties, namely the Christian Democrats, the Social Democrats, and the Green Party, characterising them as 'enemies of Türkiye'. While no evidence of covert operations has been discerned from open-source reports, the German government, led by Chancellor Angela Merkel, construed this act as an encroachment upon the sovereign prerogatives of German voters.[70]

China, on the other hand, has been active in the cultivation of incentives targeted at Chinese diasporic communities mostly in Asia and North America where it has fostered support for political candidates aligned with a pro-engagement stance towards Beijing. For instance, evidence surfaced in 2014 indicating that the Chinese Consulate in Toronto directly intervened in elections by seeking to dispatch Chinese students to influence voters in households where only the Chinese language was spoken,[71] advancing preferred candidates.

Such cases underline the practice of attempting to 'outsource' electoral intervention to intermediaries, such as Chinese associations or students, and the extent to which foreign actors are willing to intrude into domestic political processes to advance their agendas.

In reaching out to diaspora, malign foreign actors may utilise national language media. In China's case, it also utilises social media platforms, such as WeChat. These platforms are popular notably among citizens of Chinese descent who rely on them for information. Moreover, WeChat groups are a beneficial resource for Chinese political actors, in mobilising donors and volunteers, and a useful tool for intimidating critics.[72] For instance, in Australia, an anonymous and widely-shared

70 Usta, B., 'Erdogan Tells Turks in Germany to Vote against Merkel', Reuters, 18 August, 2017. Available at https://www.reuters.com/article/us-germany-Türkiye-idUSKCN1AY17Z (accessed August 2023).

71 Cooper, S., 'Is China Influencing B.C. Politicians? Falun Gong Case Points That Way', Victoria Times Colonist, 16 September, 2014. Available at https://www.timescolonist.com/bc-news/is-china-influencing-bc-politicians-falun-gong-case-points-that-way-4613703 (accessed August 2023).

72 Nuttall, J., 'Death Threats against Chinese Canadian Who Spoke out on Uyghur Genocide Claims Must Be Investigated, Say B.C. Community Leaders', Toronto Star, 14 April, 2021. Available at https://www.thestar.com/news/canada/death-threats-against-chinese-canadian-who-spoke-out-on-uyghur-genocide-claims-must-be-investigated/article_38720cec-b76b-51cf-a602-48407d6268c9.html (accessed August 2023).

letter was circulated among Chinese Australians urging them to 'take down the far-right Liberal ruling party'.[73]

The integral role of technology platforms, which are leveraged to mobilise and sway voters in novel ways, is highlighted by instances of overt manipulation. Intricate tactics encompass taking control of WeChat groups[74] and orchestrating social media campaigns that endorse particular candidates, often of Chinese origin. These instances, however, are not limited only to China and underscore a broader pattern of manipulation observed globally.[75]

### Box 2: Using WeChat to recruit a candidate acceptable to China

Country(ies) affected: Canada

What happened: In August and September 2022, the Chinese Vancouver Consulate utilised WeChat to recruit a candidate who could garner support from the Chinese community. This was in opposition to Brad West, the Mayor of Port Coquitlam and a vocal critic of China in Canadian politics, during the run-up to British Columbia's 2022 municipal elections. Prior to this, West claims he had been targeted through WeChat messages portraying him as anti-Chinese, racist, and a promoter of the US agenda in Canada.

How it was detected: The case came to light when Brad West reported it to the media a year later, in August 2023. He arguably had evidence regarding the matter, provided by the Canadian Security Intelligence Service (CSIS).

Why it matters: This case exemplifies how social media platforms, such as WeChat, can be employed by foreign state actors to try to connect with diasporic communities abroad and undermine local politicians with critical stances against the intervener.

Source: Cooper, S., 'Exclusive: Beijing Allegedly Tried to Run Candidate against Popular Canadian Mayor', The Bureau, 23 August, 2023. Available at https://www.thebureau.news/p/exclusive-beijing-allegedly-tried?utm_campaign=post (accessed August 2023).

It is crucial to avoid prematurely assuming that all interactions between the state of origin and diasporic communities are malicious and, even when they are, that they will inevitably yield the intended results. Quite the opposite, these endeavours can sometimes lead to unforeseen

73 O'Malley, N., Joske. A., 'Mysterious Bennelong Letter Urges Chinese Australians to "take down" the Turnbull Government', The Sydney Morning Herald, 13 December, 2017. Available at https://www.smh.com.au/politics/federal/mysterious-bennelong-letter-urges-chinese-australians-to-take-down-the-turnbull-government-20171213-h03pc4.html (accessed August 2023).

74 Connolly, A., 'Trudeau Says Using Minister's WeChat Group to Fund Lawsuit against Journalist Was "Unacceptable"', Global News, 16 May, 2020. Available at https://globalnews.ca/news/6986602/joyce-murray-wechat-china-lawsuit/ (accessed August 2023).

75 Mosk, M., Turner, T., Faulders, K., 'Russian Influence Operation Attempted to Suppress Black Vote: Indictment', 18 February, 2018. Available at https://abcnews.go.com/Politics/russian-influence-operation-attempted-suppress-black-vote-indictment/story?id=53185084 (accessed August 2023).

outcomes. This is evidenced, for instance, by the decision of the majority of Malaysian Chinese to cast their votes against Najib Tun Razak, despite China's support for his re-election.[76]

- **Buying Votes**

In their quest to interfere in elections, malign foreign actors may resort to buying votes through covert means. However, vote buying carries a significant risk as it is mostly perceived as an illicit practice. Vote buying impacts voter autonomy and leads to the establishment of dependencies. Thus, it typically involves a network of intermediary brokers who transact with voters.[77]

Moreover, the issue of vote buying extends to the concerning fact that it predominantly exploits individuals with lower income levels,[78] who tend to be more susceptible to monetary or in-kind forms of recompense, such as food, energy or medicine. In certain instances, vote buying may also strategically target apathetic voters. This underscores the multifaceted nature of such manipulative practices, which may be used by both domestic as well as foreign actors. A notable illustration of this occurred during the 2013 Iranian presidential elections, wherein an individual attempted to sell his vote on eBay. An Iranian national residing in France offered to cast his vote at the Iranian consulate in favour of a candidate chosen by the buyer for a price of EUR 99.[79]

Evidence documenting the practice of vote buying has primarily surfaced in the realm of domestic politics, [80] often involving local candidates and their brokers who provide incentives to constituents in exchange for their votes. Instances of malign foreign actors intervening in elections through vote purchases are relatively scarce within open-source materials.

However, a notable exception that unfolded in 2018 in Richmond, Canada, not only deviates from this pattern but also serves as a particularly illustrative case. In the run-up to the municipal election, the Wenzhou Friendship Society's WeChat group extended a USD 20 'transportation subsidy' as an enticement for Canadian Chinese to cast their votes, [81] despite Canadian regulations banning offers of money or rewards for voting and imposing severe penalties for misconduct. Moreover, the group provided a list of recommended candidates. The message disappeared after the society learned it had been investigated. In this particular case, China

76 Kurlantzick, J., 'China's War for Hearts and Minds', Washington Monthly, 3 March, 2023. Available at http://washingtonmonthly.com/2023/03/03/chinas-war-for-hearts-and-minds/ (accessed August 2023).

77 Joseph, O., Vashchanka, V., *Vote Buying: International IDEA Electoral Processes Primer 2*, International Institute for Democracy and Electoral Assistance (International IDEA), 2022. Available at https://www.idea.int/publications/catalogue/vote-buying (accessed August 2023).

78 See e.g. Jensen, P.S., Justesen, M.K., 'Poverty and Vote Buying: Survey-Based Evidence from Africa', *Electoral Studies*, Vol. 33, March 2014, pp. 220–232.

79 The Observers - France 24, 'An Iranian Tries to Sell His Vote on EBay', The Observers - France 24, 14 June, 2013. Available at https://observers.france24.com/en/20130614-iranian-tries-sell-vote-ebay (accessed August 2023).

80 In the European context, see e.g. Allina-Pisano, J., 'Social Contracts and Authoritarian Projects in Post-Soviet Space: The Use of Administrative Resource', *Communist and Post-Communist Studies*, Vol. 43, No. 4, 1 December, 2010, pp. 373–382; and Mares, I., Muntean, A., Petrova, T., 'Pressure, Favours, and Vote-Buying: Experimental Evidence from Romania and Bulgaria', *Europe-Asia Studies*, Vol. 69, No. 6, 3 July, 2017, pp. 940–960.

81 Mackin, B., 'Update: Vancouver City Hall Refers WeChat Vote-Buying Scheme to Police', The Breaker, 12 October, 2018. Available at https://thebreaker.news/news/wechat-wenzhou/ (accessed August 2023).

strategically employed its financial influence to bolster specific candidates participating in lower-level (municipal) elections. This strategy involved not only the utilisation of formal channels such as diplomatic missions but also the leveraging of informal connections within the Chinese diasporic community in Canada.

### 2.1.3. Reflection

Leveraging financial resources as a method for intervening in elections, whether it involves direct funding of political campaigns, parties, or individual politicians, purchasing votes, or incentivising diasporic communities to rally behind a particular candidate, undoubtedly ranks among the array of tools wielded by malign foreign actors, particularly Russia and China. It is worth noting that while the representatives of various countries often refrain from divulging precise details regarding the methods employed by these actors in electoral interventions, they do acknowledge the occurrence of such attempts. Striking a delicate balance becomes imperative, as sharing too much information could inadvertently serve the intervener's purpose of eroding public trust in the electoral process. Conversely, complete non-disclosure also presents challenges, potentially hindering a country's ability to formulate an effective response and implement countermeasures.

Moreover, the instances discussed underscore an unsettling reality: that political actors in Europe are adept at circumventing regulatory frameworks. This prompts an important question regarding the effectiveness of existing regulations governing financial contributions from third countries. Connected to this issue is also the debate on the intricate dynamics of the revolving-door practice[82] in which malign foreign state and non-state actors employ former politicians shortly after they leave office.

The intricate landscape of electoral interventions, particularly those involving financial means, underscores the necessity for countermeasures to be all-encompassing and holistic. These measures should not solely address the direct avenues of financial influence but also tackle the most conspicuous structural vulnerabilities.

[82] See e.g.: McKenzie, N., Baker, R., Uhlmann, C., 'Liberal Andrew Robb Took $880k China Job as Soon as He Left Parliament', The Sydney Morning Herald, 6 June, 2017. Available at https://www.smh.com.au/national/liberal-andrew-robb-took-880k-china-job-as-soon-as-he-left-parliament-20170602-gwje3e.html (accessed August 2023); see also Bloomberg, 'China Is Said to Probe Chairman of Emerging Energy Star CEFC', 1 March, 2018. Available at https://www.bloomberg.com/news/articles/2018-03-01/cefc-chairman-ye-probed-by-chinese-authorities-caixin-reports (accessed August 2023); and US Department of Justice, Office of Public Affairs, 'Former Head of Organization Backed by Chinese Energy Conglomerate Sentenced to Three Years in Prison for International Bribery and Money Laundering Offenses' [Press Release], 25 March, 2019. Available at https://www.justice.gov/opa/pr/former-head-organization-backed-chinese-energy-conglomerate-sentenced-three-years-prison (accessed August 2023).

## 2.2. Information Manipulation

### 2.2.1. Background

Malign foreign actors have demonstrated a penchant for the manipulation of information and public opinions. Their efforts take the shape of coordinated campaigns which utilise media channels, including social media, and involve creating content designed to appear as if it originates from the target country.[83]

While the phenomenon of information manipulation is a long-standing feature of the international system[84] and is not exclusive to the internet era, developments in technology[85] have decreased the costs and widened the scope, reach and speed of information transmission. Social media provides an ability to segment audiences and target messages in a largely unregulated way.[86] The solutions offered by information technologies are becoming more elaborate: e.g., attacks aimed at amplifying geopolitical tensions have taken place where weblinks to content that initially impersonates existing news sites are later redirected to the authentic domain.[87] User vigilance and media literacy alone is falling short of countering such methods. This presents new challenges to democratic societies, as the voting calculus of their members is influenced by the information they consume.[88]

In addition to amplifying false narratives, information manipulation may involve suppression tactics such as intimidation, smear campaigns, and strategic lawsuits against public participation (SLAPPs). These methods are employed by malign foreign actors to deter journalists, researchers, or civil society actors from disseminating unfavourable information or shining a light on their activities, methods, and networks.

The information manipulation activities of malign foreign actors can influence voting behaviour in liberal democracies in both narrow and broad ways. Narrow practices involve targeting specific populations during election periods and focusing on topics relevant to the political debate. On the other hand, broader practices entail feeding into popular anxieties, amplifying polarised narratives, and dehumanising certain social groups. For example, a Russian information

83 Martin, D.A., Shapiro, J.N., Ilhardt, J.G., 'Online Political Influence Efforts Dataset, Version 4.0', 24 March, 2023. Available at https://esoc.princeton.edu/publications/trends-online-influence-efforts (accessed August 2023).

84 Bennett, W. L., Livingston, S., eds., *The Disinformation Age: Politics, Technology, and Disruptive Communication in the United States*, 1st ed., Cambridge University Press, Cambridge, 2020, p. 171.

85 Jung, H.M., 'Information Manipulation Through the Media', *Journal of Media Economics*, Vol. 22, No. 4, 30 November, 2009, pp. 188–210.

86 Bradshaw, S., Howard, P.N., *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation*, Working Paper, Oxford, 2018. Available at https://demtech.oii.ox.ac.uk/research/posts/challenging-truth-and-trust-a-global-inventory-of-organized-social-media-manipulation/ (accessed August 2023).

87 Bradshaw, S., Howard, P.N., *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation*, Working Paper, Oxford, 2018. Available at https://demtech.oii.ox.ac.uk/research/posts/challenging-truth-and-trust-a-global-inventory-of-organized-social-media-manipulation/ (accessed August 2023).

88 Brennan, G., Lomasky, L., eds., 'The Logic of Electoral Choice', *Democracy and Decision*, 1st ed., Cambridge University Press, Cambridge, 1993, pp. 19–31.

manipulation campaign spread disinformation about the bad behaviour of Ukrainian displaced persons in Europe,[89] illustrating the wider impact of such tactics.

EU member states are increasingly adopting approaches to counter digital information manipulation. According to mapping of exercised solutions conducted by the European Regulators Group for Audiovisual Services, two approaches have emerged among the EU members. The first group, which includes Croatia, France, and Lithuania, has adopted legislative acts containing 'statutory regulations with a specific definition of fake news, information manipulation, and disinformation'.[90] The second group, which includes Estonia, Poland, Denmark, Italy, Finland, and Spain, among others, exercises varying 'non-legislative, but state-coordinated approaches, where the documents have no legal binding force, but the state played an integral part in the creation of the conceptual elements'.[91] The Law N. 2018-1202 relating to the fight against the manipulation of information[92] passed in France following the final reading by the National Assembly in December 2018 specifically tackles information manipulation during electoral campaigns. Still, researchers point out that 'the scope of the new legislation against the manipulation of information, constrained by the freedom of expression, remains modest,'[93] essentially leaving the country's electoral environment vulnerable to malign foreign influence. The 2020 Inquiry of the Intelligence and Security Committee of the UK Parliament acknowledged that the existing division of responsibilities within the government, as well as the legislative framework, lacks the capability to deter and counter such attacks on the British information space. Efforts to address the problem also include exploring technological solutions, such as a platform-agnostic machine learning approach to detect content involved in coordinated influence operations.[94] While this tool may prove valuable for safeguarding the electoral environment in the future, it's essential to recognise that it's not a cure-all solution.

89 Neidhardt, A.H., *Disinformation on Refugees from Ukraine: Boosting Europe's Resilience after Russia's Invasion*, Foundation for European Progressive Studies (FEPS), 2022. Available at https://feps-europe.eu/wp-content/uploads/2022/12/PS-Disinformation.pdf (accessed August 2023).

90 European Regulators Group for Audiovisual Media Services (ERGA), *Notions of Disinformation and Related Concepts*, ERGA, 2020, p. 62. Available at https://erga-online.eu/wp-content/uploads/2021/03/ERGA-SG2-Report-2020-Notions-of-disinformation-and-related-concepts-final.pdf (accessed August 2023).

91 European Regulators Group for Audiovisual Media Services (ERGA), *Notions of Disinformation and Related Concepts*, ERGA, 2020, p. 62. Available at https://erga-online.eu/wp-content/uploads/2021/03/ERGA-SG2-Report-2020-Notions-of-disinformation-and-related-concepts-final.pdf (accessed August 2023).

92 LOI N° 2018-1202 Du 22 Décembre 2018 Relative à La Lutte Contre La Manipulation de l'information (1). Available at https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037847559 (accessed August 2023).

93 Couzigou, I., 'The French Legislation Against Digital Information Manipulation in Electoral Campaigns: A Scope Limited by Freedom of Expression', *Election Law Journal: Rules, Politics, and Policy*, Vol. 20, No. 1, 1 March, 2021, pp. 98–115.

94 Alizadeh, M., Shapiro, J.N., Buntain, C., Tucker, J.A., 'Content-Based Features Predict Social Media Influence Operations', *Science Advances*, Vol. 6, No. 30, 24 July, 2020.

The following sub-chapter describes several types of information manipulation. In concrete cases it demonstrates methods employed by various malign foreign actors and outlines the European vulnerabilities associated with each form of information manipulation.

### 2.2.2. Methods

- **Media and social media campaigns**

Malign foreign actors have recognised the immense power of media and social media platforms as tools for manipulating public sentiment before elections. They employ targeted campaigns that exploit the vulnerabilities of these platforms (such as embedded biases or functioning of algorithms) to disseminate propaganda, amplify divisive narratives, and exploit emotional triggers.[95]

Coordinated influence operations conducted by malign foreign governments or foreign state-backed entities often involve deploying deceptive tactics to make their messages appear authentic to the target audience. Clumsy and non-native wording of articles, social media posts, and Internet memes has, in many cases, helped researchers and journalists, as well as the wider public to establish inauthentic behaviour originating from abroad. Today, the evolution of AI-powered tools including DeepL, and language models ChatGPT, and Bard, provide constantly developing text generation, translation, and improvement solutions, imbuing the messages with indigenous qualities, and obfuscating the source.

Intentional obfuscation makes it difficult for authorities and platforms to accurately attribute responsibility for spreading false narratives and disinformation. A case in point is the claim that suggested a network of Russian non-state actors, involving organised crime, coordinated and executed a cyber information manipulation campaign on behalf of the Russian state. The campaign's objective was to influence British voters in favour of the United Kingdom leaving the EU during the 2016 referendum. However, the Report of the Intelligence and Security Committee of the UK Parliament did not provide conclusive evidence to support this claim, whilst some data was withheld, supposedly for information protection purposes.[96] The lack of clear attribution can hinder effective countermeasures, allowing the manipulation to persist and potentially undermine democratic processes, social cohesion, and public trust in the media.

95 Starr, P., 'The Flooded Zone: How We Became More Vulnerable to Disinformation in the Digital Era', in Bennett, W.L., Livingston, S. (eds.), *The Disinformation Age*, 1st ed., Cambridge University Press, Cambridge, 2020, p. 80.

96 Intelligence and Security Committee of the UK Parliament, 'Russia', 21 July, 2020, p. 2. Available at https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf (accessed August 2023).

### Box 3: The RRN Case as an example of typosquatting

Country(ies) affected: France, Germany, the United Kingdom, Latvia, Estonia, Ukraine, Italy, United Arab Emirates, Israel, the United States

What happened: Pro-Russian narratives to undermine Western support to Ukraine were disseminated via a digital media campaign. The content was spread through typosquatting (i.e., a registration of a common misspelling of another organisation's domain as their own) and cloning of popular media sites, including at least 58 articles of Le Monde, 20Minutes, Le Parisien and Le Figaro and amplified through inauthentic Facebook and Twitter (now X) user networks.

How it was detected: The French Vigilance and Protection against Foreign Interference (VIGINUM) service identified a digital campaign to manipulate information that has targeted several European countries since September 2022, including France. EU DisinfoLab had previously reported on similar actions elsewhere in Europe, with such media as Bild, Ansa, The Guardian or RBC Ukraine being typosquatted. The company META named the Russian enterprises Social Design Agency (ASP) and Struktura to be behind the coordinated inauthentic behaviour.

Why it matters: Although these clone sites have been shut down, the scandal has not disabled the activities of the alleged perpetrator. The Social Design Agency (ASP) is still active, lists several Russian ministries and municipalities among its clients, and continues to offer through its 'platforms for capturing the Internet space' services such as 'audience involvement in the customer's initiatives, formation of a network of "brand advocates", activity monitoring, early detection of information threats in social networks, control of the "grey" (deep) Internet.' The method of typosquatting itself can be easily replicated and perfected, and topics can be changed to influence European voters during elections.

Source: Secretariat-General for National Defence and Security, *RNN: A Complex and Persistent Digital Information Manipulation Campaign*, 19 July, 2023, p.17. Available at https://www.sgdsn.gouv.fr/files/files/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN1.pdf (accessed August 2023); Alaphilippe, A., Machado, G. Miguel, R., Poldi, F., 'Doppelganger - Media Clones Serving Russian Propaganda', EU DisinfoLab, 27 September, 2022. Available at https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf (accessed August 2023); Meta, 'Removing Coordinated Inauthentic Behavior From China and Russia, 27 September, 2022. Available at https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/ (accessed August 2023); Sp-agency.ru, 'ДИГИТАТОР', Available at https://sp-agency.ru/tools/9/ (accessed August 2023).

EU institutions have been aware of Russian information manipulation campaigns at least since 2015, when the East StratCom established the EUvsDisinfo platform,[97] whereas other malign foreign actors have been recognised at a slower pace. While Russia is responsible for 61 % of documented political influence efforts using information manipulation (March 2023 data), the

97 EUvsDisinfo, 'Election Meddling and Pro-Kremlin Disinformation', 2019. Available at https://euvsdisinfo.eu/uploads/2019/10/PdfPackage_EUvsDISINFO_2019_EN_V2.pdf (accessed August 2023).

origins of the remaining 39 % can be attributed to other countries: primarily China, Iran, Saudi Arabia, and the United Arab Emirates.[98]

Though China has become increasingly more active in information manipulation in the Western space,[99] its attempts have not reached the scope, intricacy, and yield of the Russian campaigns. This is, perhaps, due to the fact that China had concentrated its efforts on innovation in high-tech social control, whereas Russia had been weaponising information technologies as part of targeted influence operations.[100] China-affiliated actors use media and social media campaigns to primarily 'present China's authoritarian regime as benign, to promote China as a model for governance and information management in developing countries, (…) to encourage openness to Chinese financing and investment, (…) suppress criticism of the country's domestic policies and the activities of China-linked entities abroad, and to win foreign policymakers' vocal support for the regime's positions.'[101]

Russia, on the other hand, sees the ongoing information environment as a battleground with the West and speaks of it in the vocabulary of an armed conflict that it must win. Artem Sheikin, member of the Russian Federation Council Committee on Constitutional Legislation and State Construction, writes: 'We are resisting the West's growing information pressure with dignity, but we will still have to go on the offensive ourselves to win the cyber war.'[102] Russia's aims include weakening liberal democratic societies, undermining the role of Western powers in the world, discrediting supranational institutions including NATO and the EU.[103] To this end, malign actors acting at the behest of the Russian state artificially enhance 'a trend, a consensus, a hashtag,

98 Martin, D.A., Shapiro, J.N., Ilhardt, J.G., 'Online Political Influence Efforts Dataset, Version 4.0', 24 March, 2023. Available at https://esoc.princeton.edu/publications/trends-online-influence-efforts (accessed August 2023).

99 Merchant, N., Lee, M., 'US Sees China Propaganda Efforts Becoming More Like Russia's', AP News, 7 March, 2023. Available at https://apnews.com/article/china-russia-intelligence-foreign-influence-propaganda-0476f41aa932cd4850627a7b8984baa2 (accessed August 2023).

100 Polyakova, A., Meserole, C., *Exporting Digital Authoritarianism: The Russian and Chinese Models, Brookings Institution,* 2019, p. 2. Available at https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf (accessed August 2023).

101 Cook, S., 'Countering Beijing's Media Manipulation', *Journal of Democracy*, Vol. 33, No. 1, 2022, pp. 116–130.

102 Sheikin, A., ‚Информационная война', council.gov.ru, 21 June, 2022. Available at http://council.gov.ru/services/discussions/blogs/136503/ (accessed August 2023).

103 Duberry, J., '"Dezinformatsiya" and Foreign Information Manipulation and Interference', Global Challenges, May 2023. Available at https://globalchallenges.ch/issue/13/dezinformatsiya-and-foreign-information-manipulation-and-interference/ (accessed August 2023).

a public figure, a piece of news, a view of the truth'[104] without necessarily advocating a specific position or taking sides.[105]

Alarmingly, media and social media information manipulation campaigns can have far-reaching and lasting consequences that go beyond the immediate goals of swaying or confusing public opinions. One of the significant long-term effects is the erosion of societal trust in democratic institutions and processes surrounding elections. These campaigns specifically target the undermining of confidence in ballot counting procedures, election officials responsible for the process, and alternative voting methods, such as electronic or mail voting. By sowing doubt and suspicion about the integrity of the electoral system, these actors can weaken the foundations of democratic governance, creating instability and division within societies. The European Union has a unique fragility in this regard due to the challenge of not only safeguarding trust in national elections, but also tackling the perception of democracy deficit at the EU level.

### Box 4: The META Czech case

Country(ies) affected: Czechia, the United States

What happened: In 2022, networks originating from China and Russia were implicated in an influence operation targeting US domestic politics ahead of the midterm elections, as well as Czechia's foreign policy toward China and Ukraine. The Chinese network specifically targeted Czechia with a message 'criticising the state's support of Ukraine in the war with Russia and its impact on the Czech economy, using the criticism to caution against antagonising China'.

How it was detected: The case was uncovered by the META research team.

Why it matters: Although this particular content was removed, META admits that the method can be easily replicated, and topics can be tweaked to influence European voters during elections.

Source: Nimmo, B., Torrey, M., 'Taking down Coordinated Inauthentic Behavior from Russia and China', Meta, September 2022. Available at https://www.politico.eu/wp-content/uploads/2022/09/27/NEAR-FINAL-DRAFT-CIB-Report-ChinaRussia-Sept-2022.pdf (accessed August 2023); Meta, 'Removing Coordinated Inauthentic Behavior From China and Russia', 27 September, 2022. Available at https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/ accessed August 2023).

104 Duberry, J., '"Dezinformatsiya" and Foreign Information Manipulation and Interference', Global Challenges, May 2023. Available at https://globalchallenges.ch/issue/13/dezinformatsiya-and-foreign-information-manipulation-and-interference/ (accessed August 2023).

105 Ellehuus, R., 'Mind the Gaps: Russian Information Manipulation in the United Kingdom', Center for Strategic and International Studies, 31 January, 2020. Available at https://www.csis.org/analysis/mind-gaps-russian-information-manipulation-united-kingdom (accessed August 2023).

- **Disinformation**

Disinformation constitutes 'all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit.'[106] The activities of malign foreign actors fall into the first category, as they aim to confuse voters, distort the truth, and manipulate electoral outcomes by disseminating false information through various channels, including social media, websites, and news outlets. The appeal of this tactic to malign foreign actors seeking to interfere in elections can be attributed to several factors. First, the founding characteristics of liberal democratic societies, such as freedom of speech, plurality of opinion, a decentralised and independent media landscape, and civil society participation can be weaponised by injecting and fuelling false information. Secondly, research has shown that false news spreads online more pervasively than the truth.[107] Thirdly, social media platforms, driven by the goal of maximising scale and advertising revenue, employ algorithms designed to boost engagement, which often facilitates the spread of disinformation through emotionally charged news stories.[108] Disinformation actions do not have to directly target voters to be able to influence voting behaviour. Injecting disinformation into public opinion and capitalising on existing societal tensions can influence voting behaviour, leading to affective polarisation[109] and more contrasting electoral choices among voters.

Disinformation campaigns conducted by malign foreign actors in the European Union and its member states 'undermine the political process through the use of various forms of malicious fabrications, infiltration of grassroots groups, and automated amplification techniques.'[110] In a multi-faceted effort to cater to both extreme sides of the political spectrum, mainly Russia,[111, 112]

106 European Commission, Directorate-General for Communications Networks, Content and Technology, *A multi-dimensional approach to disinformation – Report of the independent High level Group on fake news and online disinformation*, Publications Office, 2018, Available at https://data.europa.eu/doi/10.2759/739290 (accessed August 2023).

107 Vosoughi, S., Roy, D., Aral, S., 'The Spread of True and False News Online', *Science*, Vol. 359, No. 6380, 9 March, 2018, pp. 1146–1151. Available at https://www.science.org/doi/10.1126/science.aap9559 (accessed August 2023).

108 Starr, P., 'The Flooded Zone: How We Became More Vulnerable to Disinformation in the Digital Era', in Bennett, W.L., Livingston, S. (eds.), *The Disinformation Age*, 1st ed., Cambridge University Press, Cambridge, 2020, p. 80.

109 Serrano-Puche, J., 'Digital Disinformation and Emotions: Exploring the Social Risks of Affective Polarization', *International Review of Sociology*, Vol. 31, No. 2, 4 May, 2021, pp. 231–245.

110 European Commission, Directorate-General for Communications Networks, Content and Technology, *A multi-dimensional approach to disinformation – Report of the independent High level Group on fake news and online disinformation*, Publications Office, 2018, p. 10. Available at https://data.europa.eu/doi/10.2759/739290 (accessed August 2023).

111 US Department of Justice, 'Report on The Investigation into Russian Interference in the 2016 Presidential Election', Volume I of II, March 2019, p.14. Available at https://www.justice.gov/archives/sco/file/1373816/download (accessed August 2023).

112 Belton, C., Harris, S., Mekhennet, S., 'Kremlin Tries to Build Antiwar Coalition in Germany, Documents Show', Washington Post, 21 April, 2023. Available at https://www.washingtonpost.com/world/2023/04/21/germany-russia-interference-afd-wagenknecht/ (accessed August 2023).

but also Chinese[113] state-affiliated actors are engaged in securing the support of those publics sympathetic to far-right and far-left political forces through information manipulation methods. Different, at times contradictory, disinformative content is spread, tailored to strongly resonate with sympathisers of each political extreme. A report by the US State Department urged governments to guard against covert political financing 'not just by Russia, but also by China and other countries imitating this behaviour.'[114]

Still, one should note that for the time being Russian and Chinese disinformation activities tend to pursue different goals. Russia-backed disinformation operations seek to actively influence the political landscape, tilt public opinions, undermine trust in democratic processes and feed polarising opinions via an approach seeking to confound, not convince.[115] Similar to the mindset described in the section on media and social media campaigns, China's current disinformation approach in Europe seeks more to convince, not confound. Firstly, China aims to improve its image among Europeans by amplifying China-sympathetic narratives and disseminating pro-China propaganda, including the fair treatment of the Uyghur minority, countering claims of territory overtake in the East and South China seas, and the inevitability of unification with Taiwan. Secondly, China aims to worsen the image of the US in Europe and drive a geopolitical wedge in the transatlantic partnership.[116] To this end, Chinese state-affiliated actors have engaged in endorsing Russian disinformation on the 'US biolabs in Ukraine.'[117] In some cases, the two aims of China-originating disinformation overlap, e.g., the claim that COVID-19 originated in the US, not China.

Disinformation spread by malign foreign actors has proven to constitute a serious threat to the European election landscape. China, unlike Russia, as a foreign state actor has not yet evolved to be a strong player in disinformation weaponisation during elections in Europe. Still, given Beijing's interest in weakening the US-EU relationship coupled with its track record of amplifying some of Russia's disinformation, it has the potential to develop into a serious threat. Also, other state actors, including Iran, have been flagged for promoting disinformation in liberal democracies,

113 Karásková, I., *Analysing China Radio International's Tactics: A Case Study of Narratives Disseminated in the Czech Republic*, The Central European Digital Media Observatory (CEDMO), June 2023, p. 4. Available at https://cedmohub.eu/wp-content/uploads/2023/06/EN_Espresso.pdf (accessed August 2023).

114 Wong, E., 'Russia Secretly Gave $300 Million to Political Parties and Officials Worldwide, US Says', The New York Times, 13 September, 2022. Available at https://www.nytimes.com/2022/09/13/us/politics/russia-election-interference.html (accessed August 2023).

115 Grimes, D. R., 'Russian Misinformation Seeks to Confound, Not Convince', Scientific American, 28 March, 2022. Available at https://www.scientificamerican.com/article/russian-misinformation-seeks-to-confound-not-convince/ (accessed August 2023).

116 Bērziņa-Čerenkova, U.A., Ferrari, E., Voo, J., 'Inflaming Transatlantic Tensions? China's Public Diplomacy Efforts to Influence EU-US Relations', in Rühlig, T. (ed.), *China's Digital Power*, Digital Power China research consortium (DPC), 2022, pp. 65–74.

117 CGTN, 'China Urges US to Disclose More Details about Biolabs in Ukraine', 8 March, 2022. Available at https://news.cgtn.com/news/2022-03-08/China-urges-U-S-to-disclose-details-about-biolabs-in-Ukraine-18eA7VpwQRG/index.html (accessed August 2023).

including in Israel and the US. Therefore, the EU is under the risk of being targeted by a growing number of foreign state-affiliated disinformation actors.

### Box 5: The case of COVID-19 origins

Country(ies) affected: global

What happened: In March 2020, the spokesperson of the Chinese Ministry of Foreign Affairs, Zhao Lijian, posted several messages on the Twitter (now X) platform stating that 'it might be the US army who brought the epidemic to Wuhan' and called for an explanation from the US. The following day, he retweeted a link to a report with the comment 'Further Evidence that the Virus Originated in the US.'

Why it matters: The case demonstrates that Chinese state actors intentionally spread disinformation pertaining to a subject of global significance. Given China's emphasis on discursive power, there is a growing network of Chinese state-affiliated actors in the European information space, including social media, whose task it is to amplify such disinformation.

Source: Zhao, L. 赵立坚 [@zlj517], 'CDC Was Caught on the Spot. When Did Patient Zero Begin in US? How Many People Are Infected? What Are the Names of the Hospitals? It Might Be US Army Who Brought the Epidemic to Wuhan. Be Transparent! Make Public Your Data! US Owe Us an Explanation!' [Tweet], Twitter (now X), 12 March, 2020. Available at https://twitter.com/zlj517/status/1238111898828066823?lang=en (accessed August 2023); Zhao, L. 赵立坚 [@zlj517], 'This Article Is Very Much Important to Each and Every One of Us. Please Read and Retweet It. COVID-19: Further Evidence That the Virus Originated in the US.' [Tweet], Twitter (now X), 13 March, 2020. Available at https://Twitter.com/zlj517/status/1238269193427906560 (accessed August 2023).

- **Smear campaigns**

Malign foreign actors engage in smear campaigns to discredit political opponents and destabilise democratic processes. These campaigns involve spreading false or damaging information about candidates through various channels, including traditional media, social media platforms, and anonymous online forums. By tarnishing reputations and manipulating public perceptions, these actors aim to influence electoral outcomes in their favour. In most cases a smear campaign is launched by entities with resources, including authoritarian governments with captured state media outlets, as a distraction and silencing measure.[118]

Russia has been prominent in successfully executing smear campaigns targeting European politicians,[119] surpassing other actors like China. Nevertheless, it is important to note that China-connected actors also utilise this method for their purposes. Tactics aimed at critics of the Chinese government include cyber abuse, DDoS attacks, phishing, hacking, and exposing private

118 Day, J., 'What Is a Smear Campaign? Can You Spot and Beat One?', Liberties.Eu, 28 March, 2023. Available at https://www.liberties.eu/en/stories/smear-campaign/44721 (accessed August 2023).

119 Keating, D., 'EFDD 'Smear Campaign' Used Russian Help', POLITICO, 29 January, 2015. Available at https://www.politico.eu/article/efdd-smear-campaign-used-russian-help/ (accessed August 2023).

information about family members. In some cases, curiously, attacks originating from China have achieved the opposite objective. The candidate in fact gained notoriety and support at home after being subjected to Chinese criticism, as seen in the case of Lithuanian politicians who have been driving a deeper Lithuanian engagement with Taiwan.[120] Still, these campaigns appear to be more efficient if they are aimed at Chinese nationals or Chinese descendants living abroad and utilise the Chinese language online space. A character assassination campaign targeting a Canadian journalist contained online posts in Chinese accusing her of numerous sexual liaisons, prostitution, spying for the Chinese government, and embezzling political dissidents' funds, as well as doctored photos and advertisements for escort services, using her face and personal details.[121]

Smear campaigns backed by malign foreign actors pose a great threat to the European election landscape for the reasons of accessibility and efficiency. Authoritarian governments, unlike the targeted party, can make use of an asymmetry in resources, making it difficult for the targeted individuals to avert accusations. They also utilise news production patterns which prioritise fast news capturing the audience's attention to verification of news origin. Especially in the run-up to an election, a smear campaign may play a decisive role. In 2016, Moscow's disinformation campaigns targeting Hillary Clinton, readily picked up by local pundits,[122] were a strong factor contributing to her defeat in the US presidential election.

120 Global Times, 'Lithuanian Politicians, Nathan Law Are West's Tools to Do "Dirty Work"', 24 November, 2021. Available at https://www.globaltimes.cn/page/202111/1239862.shtml (accessed August 2023).

121 Wang, Y., 'China's Overseas Critics under Pressure from Smear Campaigns, Cyber Attacks', Committee to Protect Journalists, 11 March, 2016. Available at https://cpj.org/2016/03/chinas-overseas-critics-under-pressure-from-smear/ (accessed August 2023).

122 Benkler, Y., Faris, R., Roberts, H., *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*, Oxford University Press, New York, 2018, p.147.

### Box 6: The Vystrčil case

Country(ies) affected: Czechia

What happened: A Swiss organisation that 'cooperates with the China News Service, which is directly under the United Front Work Department' approached a Czech media outlet with the claim that the Czech Senate President Miloš Vystrčil had received a 'clandestine payment of USD 4 million for his historic visit [to Taiwan] from the Taiwanese to be used for a future presidential campaign.'

How it was detected: The management of Swiss consultancy RefinSol Advisory Services sent an appeal to the editorial offices of Czech media outlet Aktuálně.cz, urging them to publish the material. The CEO, executive assistant and CFO of RefinSol Advisory Services Zhu Ailian, Robert J. Mojzes, Michael Winkler are also listed as CEO, executive assistant and the chairman of the outlet EurAsia Info known for spreading pro-China content. The appeal included a link to a related French news site. Aktuálně.cz conducted their own investigation, found no proof to the claim, and exposed the China link of the source.

Why it matters: Defamatory material is easy to produce and inexpensive to distribute. If the online media outlet approached by an entity acting on behalf of a malign foreign actor does not have sufficient in-house investigative capacity to follow up on the claims, or has a particular bias against a political figure, such defamatory claims can reach the public space and inflict irreparable reputational damage on the person targeted.

Source: Valášek, L., Truchlá, H., '"Four Million for Vystrčil": Chinese Attempt at Disparaging President of Czech Senate - Aktuálně.Cz', Aktuálně, 11 November, 2020. Available at https://zpravy.aktualne.cz/domaci/four-million-dollars-for-vystrcil-chinese-attempt-at-dispara/r~1808fbea245111eb95caac1f6b220ee8/ (accessed August 2023); Weber, R., *Unified message, rhizomatic delivery. A preliminary analysis of PRC/CCP influence and the united front in Switzerland,* Sinopsis – China in Context and Perspective, 2020, pp. 2, 31.

- **Stakeholder data scraping**

Data scraping does not qualify as active information manipulation, since the act of scraping itself does not influence the decision-making of an individual or a group. Data scraping is a neutral method, and as such can also be helpful to investigative journalists.[123] Still, as information gathering is the first phase of a successful, tailored and targeted manipulation, malign foreign actors' activities in this field should not be overlooked.

Scraping is a powerful and widespread marketing tool, operating under the premise that accessing, storing, bulking, and analysing openly available data, including personal data, is legal, since the individuals have placed the data into the public domain themselves. However, often the individual is not aware of the amount of data they are leaving behind, including geotags and other metadata. If several sources are compiled, a file containing ample information about an individual can be produced, including pictures, videos, location, telephone numbers, work

123 Bradshaw, P., 'Data Journalism', in Craig, D., Zion, L. (eds.), *Ethics for Digital Journalists: Emerging Best Practices*, Routledge, New York, 2015.

information, and details of family members. If data scraping for marketing purposes is a business practice that uses the information to increase commercial targeting success rates, including through targeted ads, then stakeholder data scraping pursues a different, political goal. It aims to compile namelists, supplemented with contact and personal information, and the creation of a database that can serve the interests of a malign foreign state actor, including in election and candidate manipulation.

Data scraping is also the first step towards doxxing, i.e., revealing personal information online in a campaign of abuse and intimidation. This tactic has been used by authoritarian governments in Europe, including Russia, to silence their critics.[124] If compromising information is uncovered during scraping, malign foreign actors can use it to engage in blackmail.

Data scraping conducted on behalf of malign foreign actors poses a threat to the European election landscape as it is a legal, affordable, accessible and in most cases untraceable instrument that can lead to grooming, doxxing or blackmail of political candidates or public figures.

### Box 7: The Zhenhua Data Information Technology case

Country(ies) affected: nearly 200 countries/territories worldwide, including European countries

What happened: In 2020, a China-based company with reported links to the Chinese military and government was exposed for scraping and storing open-source online data on millions of users from around the world, including European politicians.

How it was detected: The issue was first reported by the academic Christopher Balding, then disseminated through an international media consortium.

Why it matters: Open-source data scraping is a thriving industry. It is a tool for online businesses to keep up with their competitors and is not fully outlawed in the EU or US, provided copyright or private data infringement does not take place. It is therefore an accessible, inexpensive and effective means for authoritarian governments to pursue their objectives of information gathering, weaponisation, and intimidation, constituting a high risk for election manipulation.

Source: Hurst, D., Kuo, L., Graham-McLay, C. 'Zhenhua Data Leak: Personal Details of Millions around World Gathered by China Tech Company', The Guardian, 14 September, 2020. Available at https://www.theguardian.com/world/2020/sep/14/zhenhua-data-full-list-leak-database-personal-details-millions-china-tech-company (accessed August 2023); Brady, A.-M., 'The Data Dump That Reveals the Astonishing Breadth of Beijing's Interference Operations', Washington Post, 26 September, 2020. Available at https://www.washingtonpost.com/opinions/2020/09/26/data-dump-that-reveals-astonishing-breadth-beijings-interference-operations/ (accessed August 2023); Balding, C., Potter, R., et al., 'Chinese Open Source Data Collection, Big Data, And Private Enterprise Work For State Intelligence and Security: The Case of Shenzhen Zhenhua', Rochester, NY, 13 September, 2020. Available at https://ssrn.com/abstract=3691999 (accessed August 2023).

124 Yates, W., 'Jessikka Aro: How pro-Russian Trolls Tried to Destroy Me - BBC News', BBC News, 6 October, 2017. Available at https://www.bbc.com/news/blogs-trending-41499789 (accessed August 2023).

- **Strategic lawsuits against public participation**

SLAPPs represent an intimidation suit that menaces citizen activism,[125] as SLAPP lawsuits are often filed against activists, journalists, or civil society organisations.

Malign foreign actors have increasingly employed SLAPPs to silence critics and undermine democratic discourse before elections. Authoritarian governments including Russia, China, Türkiye, and Venezuela,[126] rely on proxy plaintiffs to file claims against investigative journalists, publishing houses, media outlets, dissidents, and exiled politicians.[127]

Russian oligarchs including Yevgeny Prigozhin,[128] Roman Abramovich,[129] and Oleg Deripaska[130] have been named among those acting on behalf of the Russian state in using SLAPPs to silence investigative research. Chinese companies have also been reported to act as proxies for the state, filing breach of contract suits against dissidents abroad, pressuring them to return to China.[131]

A proposal for a directive of the European Parliament and of the Council on protecting persons who engage in public participation from manifestly unfounded or abusive court proceedings is currently under review in the European Union. Still, until such laws are in place, SLAPP suits pose a risk for the European electoral landscape. SLAPPs enable malign foreign actors to impose costs, but also influence the popular opinion or 'rewrite history'[132] in the target country, therefore, the attacking party is not deterred by the financial losses or even the unfavourable outcome that can

125 Harper, J., 'Attorneys as State Actors: A State Action Model and Argument for Holding SLAPP-Plaintiffs' Attorneys Liable under 42 U.S.C. 1983', *UC Law Constitutional Quarterly*, Vol. 21, No. 2, 1 January, 1994, p. 405.

126 Zambrano, D. A., 'Testimony Before the US-China Economic and Security Review Commission', 4 May, 2023. Available at https://www.uscc.gov/sites/default/files/2023-05/Diego_Zambrano_Testimony.pdf (accessed August 2023).

127 Zambrano, D. A., 'Foreign Dictators in US Court', *The University of Chicago Law Review*, Vol. 89, No. 1, 1 January, 2022, pp. 157–252. Available at https://www.jstor.org/stable/pdf/27093694.pdf?casa_token=4_D13E0hpOQAAAAA:MaHwnW3qFpEOfni5IEiETwK168ag6XeG0mGqOQ_Vu2Rpf8obQKcF6vRPZYhUp44_MCHDnT-F-TBeYrtN9U3GUQva9Nq9mXvFOwtgsSRrGv0P0OMvdxMF (accessed August 2023).

128 '18 May Yevgeniy Prigozhin's SLAPP Action against Bellingcat Founder Is Struck out' [Press release], McCue Jury & Partners, 18 May, 2022. Available at https://www.mccue-law.com/yevgeniy-prigozhins-action-against-bellingcat-founder-struck-out/ (accessed August 2023).

129 'Catherine Belton, Journalist and Author of "Putin's People: How the KGB Took Back Russia and Then Took on the West"', The Foreign Policy Centre, 15 February, 2023. Available at https://fpc.org.uk/catherine-belton-journalist-and-author-of-putins-people-how-the-kgb-took-back-russia-and-then-took-on-the-west/ (accessed August 2023).

130 United States District Court, District of Columbia, 17 October, 2017, *Deripaska v. Associated Press,* 282 F. Supp. 3d 133. Available at https://casetext.com/case/deripaska-v-associated-press (accessed August 2023).

131 Zambrano, D. A., 'Testimony Before the US-China Economic and Security Review Commission', 4 May, 2023. Available at https://www.uscc.gov/sites/default/files/2023-05/Diego_Zambrano_Testimony.pdf (accessed August 2023).

132 Foreign Affairs Committee, House of Commons, 'Oral Evidence: Use of Strategic Lawsuits against Public Participation, HC 1196', 15 March, 2022, Q 21. Available at https://committees.parliament.uk/oralevidence/9907/pdf/ (accessed August 2023).

occur. As activists remain vulnerable to being strategically sued, important information affecting electoral decisions may not reach the wider European public.

### Box 8: Putin's People case

Country(ies) affected: the United Kingdom

What happened: Journalist and author Catherine Belton, and her publisher HarperCollins, encountered several legal challenges regarding a book titled 'Putin's People: How the KGB Took Back Russia and Then Took on the West', published in 2020. In 2021, four Russian oligarchs and the state-owned oil company Rosneft expressed their intention to take legal action. Four of these cases proceeded to a preliminary hearing in July 2021. During the hearing, HarperCollins settled with two Russian billionaires, Petr Aven and Mikhail Fridman, who alleged that the book contained inaccurate personal information and libel. The settlement involved making minor adjustments to specific passages in future editions, without admitting defamation. Later, regarding Rosneft's claims, three of four passages were deemed non-defamatory. Abramovich reached a settlement with HarperCollins and Belton. Minor amendments were made, and the publisher issued an apology for certain unclear aspects of the book.

Why it matters: SLAPPs on behalf of malign foreign actors are coordinated, large scale, and cost-immune. Even if the expenditures of the litigation are substantive, the plaintiffs have asymmetric advantages in the form of the financial backing from their home country. Given such asymmetry, as well as the lack of a powerful legal anti-SLAPP instrument, malign foreign actors are likely to continue to infringe upon the freedom of speech in Europe.

Source: 'Catherine Belton, Journalist and Author of "Putin's People: How the KGB Took Back Russia and Then Took on the West"', The Foreign Policy Centre, 15 February, 2023. Available at https://fpc.org.uk/catherine-belton-journalist-and-author-of-putins-people-how-the-kgb-took-back-russia-and-then-took-on-the-west/ (accessed August 2023); 'Putin's People: Settlement Reached in Roman Abramovich v HarperCollins and Catherine Belton', Corporate.Harpercollins.Co.Uk, 22 December, 2021. Available at https://corporate.harpercollins.co.uk/press-releases/putins-people-settlement-reached-in-roman-abramovich-v-harpercollins-and-catherine-belton/ (accessed August 2023).

### 2.2.3. Reflection

Information manipulation is by far the most documented and popular tool at the disposal of malign foreign actors, employing tactics such as spreading disinformation, propagating false narratives, and exploiting existing societal divisions.

Cases of information manipulation surrounding elections are methodologically diverse and employ different levels of technological sophistication, ranging from low (e.g., character assassination attempts via engineered leaks) to high (e.g., typosquatting with redirection to an

impersonated domain). Both due to the number of attempts as well as the shifting methods used for information manipulation, the role of civil society in uncovering these cases is indispensable.

In almost all major reported cases in Europe, the information first came from investigative NGOs, journalists or academics, only then leading to enquiries by national governments. Upon examining the cases of election manipulation via information, one cannot help but notice the overbearing role of public open-source research as opposed to the reports of national intelligence agencies. One can also suppose that in some cases the holders of sensitive information, including government actors, do not have the mandate to disclose their data or sources, and apply strategic targeted leaks, prompting the civil sector to disseminate the information instead.

As malign foreign actors continue to target the electoral behaviours of European civil societies, fostering an ecosystem of civil society watchdogs is crucial. This approach also coincides with the one adopted by the European External Action Service StratCom division.[133]

In some cases, information manipulation surrounding an election is a goal in itself. In other cases, however, it is only one avenue of a concerted effort at election manipulation, with other avenues such as bribery, party and candidate financing being pursued alongside. Each case needs to be established separately, and, if there is cause to believe information manipulation has taken place, it is crucial to launch a deeper investigation covering other avenues of election manipulation as well.

Legislative measures to counter information manipulation adopted and debated in several European countries, as well as on the EU level, signal rising awareness of the issue, however, they are constrained by freedom of expression principles. For instance, the Baltic states' ban of Russian state media was met with censorship accusations as Reporters Without Borders called the Baltics' decision 'a misuse of the EU sanctions policy'.[134] The accusations prompted a debate on what broadcasting falls under media opinion plurality, and what is misinformative by design.

133 European Union External Action (EEAS), *1st EEAS Report on Foreign Information Manipulation and Interference Threats*, EEAS, 2023. Available at https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en (accessed August 2023).

134 Reporters Without Borders, 'Baltic Countries: Misusing EU Sanctions to Ban Russian TV Channels Is Not a Legitimate Tool for Promoting Reliable Information', 10 July, 2020. Available athttps://rsf.org/en/baltic-countries-misusing-eu-sanctions-ban-russian-tv-channels-not-legitimate-tool-promoting (accessed August 2023).

## 2.3. Cyber-enabled electoral interference

### 2.3.1. Background

This sub-chapter delves into the intricacies of cyber threat activities as a form of electoral intervention, aiming to provide a comprehensive analysis of their nature, motivations, tactics, and potential impacts on electoral processes. By exploring real-world case studies, it seeks to enhance our understanding of this pressing issue and examine the likelihood of these TTPs being used in the European elections of 2024. The text diverges slightly from the structure observed in the preceding sub-chapters related to financial means and information manipulation. This divergence arises from the unique characteristics of cyber-enabled election interventions. It not only concentrates on methods but also sheds light on the targets and perpetrators involved in such interventions.

With the increasing reliance on digital systems and the widespread adoption of internet connectivity, electoral processes have become vulnerable to a new form of interference: cyber-enabled electoral interventions. Through sophisticated cyber operations, malign foreign actors can exploit vulnerabilities within electoral systems, aiming to undermine the integrity and legitimacy of democratic processes.

Elections are particularly vulnerable to cyber risks due to their periodic nature and the concentrated timeframe in which they occur.[135] With the exception of snap elections, they occur in regular cycles that allow for advanced planning and preparation for the attack which can be launched years before the election day. Concurrently, the voting typically takes place within a single day or extends over the duration of a few days. This places significant stress on the electoral system as it must handle a large influx of activity and data within a limited timeframe.

Cyber-enabled interventions can take various forms, including hacking into voter registration databases, tampering with vote tabulation systems, spreading malware to disrupt voting machines, or launching distributed denial-of-service (DDoS) attacks to overwhelm election websites and impede voter access to information. Such attacks not only have the potential to manipulate election outcomes but also erode public trust in the electoral process. Despite the misconception that only countries with advanced election technologies are vulnerable to cyber attacks, most elections rely in one form or another on information and communication technology (ICT) tools throughout the entire process.[136]

135 Van Der Staak, S., Wolf, P., *Cybersecurity in Elections: Models of Interagency Collaboration*, International Institute for Democracy and Electoral Assistance, 2019, p.19. Available at https://www.idea.int/publications/catalogue/cybersecurity-in-elections (accessed August 2023).

136 Van Der Staak, S., Wolf, P., *Cybersecurity in Elections: Models of Interagency Collaboration*, International Institute for Democracy and Electoral Assistance, 2019, p.12. Available at https://www.idea.int/publications/catalogue/cybersecurity-in-elections (accessed August 2023).

Globally, the incidence of cyberattacks and cyber-enabled incidents led by state actors against democratic processes is on the rise.[137] One of the most prominent examples of such interference occurred during the 2016 United States presidential election, where Russian state-sponsored hackers targeted various aspects of the electoral process. Hacking groups, linked to Russian intelligence agencies, conducted a wide array of cyber activities, including network breaches of the Democratic National Committee (DNC) and the US Democratic Congressional Campaign Committee (DCCC)[138] as well as the intrusion into voter databases and software systems.[139]

While governments such as Georgia, Ukraine or Estonia have been subjected to Russian cyberattacks at least from the mid-2000s,[140] it was the watershed moment of the 2016 US elections that brought widespread attention towards the gravity of the issue at hand. The Russian hacking into the e-mail system of the DNC served as a wake-up call for governments and policymakers worldwide, highlighting the vulnerabilities inherent in electoral systems and the urgent need for comprehensive cybersecurity measures. The attacks demonstrated the extent to which malign foreign actors could exploit digital platforms to manipulate public opinion, sow discord, and potentially sway the outcome of democratic processes. Moreover, the methods employed in these attacks exposed the complex interplay between technology and information warfare.

The US has experienced continued electoral interference since 2016. While the Russian hacking of the US elections garnered significant attention, similar incidents have been reported in other parts of the world, predominantly in Europe and in Asia-Pacific.[141] Understanding the broader context and global implications of cyberattacks on electoral processes is essential for developing effective strategies to mitigate and respond to this evolving threat landscape.

Electoral processes can face threats from adversaries beyond state actors. Non-state actors, such as organised crime groups, terrorists, hacktivist organisations, or even individual hackers, can pose significant risks to the integrity of elections through malicious cyber activities. However, the scope of this study only covers cyberattacks carried out directly by malign foreign state actors or by state-backed groups.

137 Canadian Centre for Cyber Security, 'Cyber Threat to Canada's Democratic Process', 28 February, 2019, p.32. Available at https://www.cyber.gc.ca/sites/default/files/cyber/publications/cse-cyber-threat-assessment-e.pdf (accessed August 2023).

138 FireEye, *APT28: At the Center of the Storm*, January 2017. Available at https://www.mandiant.com/resources/reports/apt28-center-storm (accessed August 2023).

139 Riley, M., Robertson, J., 'Russian Hacks on US Voting System Wider Than Previously Known', Bloomberg, 13 June, 2017. Available at https://www.bloomberg.com/politics/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections (accessed August 2023).

140 Buresh, D.L., 'Russian Cyber-Attacks on Estonia, Georgia, and Ukraine, Including Tactics, Techniques, Procedures, and Effects', *Journal of Advanced Forensic Sciences*, Vol. 1, No. 2, 19 August, 2021, pp. 15–26. Available at https://openaccesspub.org/advanced-forensic-sciences/article/1686 (accessed August 2023).

141 See Authoritarian Interference Tracker: Alliance for Securing Democracy - German Marshall Fund, 'Authoritarian Interference Tracker'. Available at https://securingdemocracy.gmfus.org/toolbox/authoritarian-interference-tracker/ (accessed August 2023).

However, attribution in the realm of cyberattacks is a complex and highly sensitive matter. Attackers employ sophisticated techniques to hide their origins, making it challenging to definitively attribute the attack to a specific entity. Ultimately, the culprit's attribution is a political decision that relies on technical aspects.[142] False flag operations, in which the true perpetrators disguise their identity, intentions, or affiliations, often by attributing the act to a different individual, organisation, or nation, present an additional challenge to attribution. For example, in a false flag operation against the headquarters of the French TV broadcaster TV5Monde, the Russian hacker group APT28, also known as Pawn Storm, posed as Islamic State militants.[143]

Certain states, such as the United States and its Five Eyes allies, display a willingness to attribute cyberattacks, while others, like France, exercise greater caution in doing so.[144] For example, while it is generally believed that the hacking group APT28 linked to the Russian GRU was responsible for the 'hack and leak' operation of Emmanuel Macron's presidential campaign, the French government never publicly attributed the meddling attempts to Russia or any other state actor.[145] Therefore, in this study, we rely on generally agreed upon assessments made by established cybersecurity companies and cybersecurity experts.

The motives behind foreign actors' cyber operations against entities involved in electoral processes may vary. The objective may be to modify the result of an election – to prevent the election of a certain candidate or a party or, on the contrary, to influence the election to the benefit of a specific candidate or campaign. However, as Delerue argues, it is highly unlikely that an outcome of an election can be changed through cyber operations.[146] Elections, even in countries with a high degree of digitisation of voting, are a series of tasks and operations which do not entirely rely on internet connection. Thus, it would require the involvement of a multitude of well-coordinated actors to influence the election in favour of a specific candidate or a political party.[147] Therefore, the actors may choose to target some parts of the electoral hardware or software to cast doubt on votes from selected electoral districts thus opening the path to possible

142 Jeangène Vilmer, J.B., *The 'Macron Leaks' Operation: A Post-Mortem*, Atlantic Council Policy, June 2019, p. 19. Available at https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf (accessed August 2023).

143 Schechner, S., 'France Says Evidence Suggests Russians Posing as Islamists Hacked Broadcaster', The Wall Street Journal, 10 June, 2015. Available at https://www.wsj.com/articles/france-says-evidence-suggests-russians-posing-as-islamists-hacked-broadcaster-1433955381 (accessed August 2023).

144 Jeangène Vilmer, J.B., *The 'Macron Leaks' Operation: A Post-Mortem*, Atlantic Council Policy, June 2019, p. 19. Available at https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf (accessed August 2023).

145 Jeangène Vilmer, J.B., Escorcia, A., Guillaume, M., Herrera, J., *Information Manipulation: A Challenge for Our Democracies*, Report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, August 2018. Available at https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf (accessed August 2023).

146 Delerue, F., *Cyber Operations and International Law*, Cambridge Studies in International and Comparative Law, Cambridge University Press, Cambridge, 2020, p. 255.

147 Delerue, F., *Cyber Operations and International Law*, Cambridge Studies in International and Comparative Law, Cambridge University Press, Cambridge, 2020, p. 255.

contestation of the entire election. Cyber operations may have more overarching and long-term goals. The intent may be to erode public trust in the fairness and integrity of elections and thus undermine the democratic institutions of the target country. Election related cyber threats can also include cyber espionage to obtain information on political stances of candidates and political parties[148] which can then be exploited for further operations, such as disinformation campaigns. Cyber espionage operations can also serve reconnaissance purposes to uncover vulnerabilities of specific information systems to facilitate future compromise of the infrastructure.

Depending on the various motivations behind the attacks, the actors resort to different methods. Observed TTPs range from DDoS and phishing campaigns to a combined method of 'hack and leak'.

### 2.3.2. Methods

- **Denial-of-Service attacks (DoS) and Distributed Denial-of-Service attacks (DDoS)**

Denial-of-Service attacks (DoS) are a less sophisticated and less common cyber threat activity. In a DoS attack, a single computer or network is used to generate a flood of traffic towards the target and can thus be blocked easily.[149] In a DDoS attack, multiple compromised computers or devices, often forming a botnet, are coordinated to simultaneously send a flood of traffic to overwhelm the target making it more difficult to defend against the attack. A successful DDoS attack can disrupt critical election services, leading to the unavailability of voter registration databases, online voting systems or election information portals. For example, in October 2017, the website of the Czech Statistical Office was taken down by a DDoS attack on the second day of elections.[150] Even though the impact of DDoS on directly influencing election outcomes is limited, they can undermine public confidence, impede voter participation, and potentially disenfranchise eligible voters. Additionally, DDoS attacks can impair access to essential information, hindering voters' ability to make informed decisions. Attackers may strategically orchestrate DDoS attacks to create the perception of electoral irregularities, manipulate public trust, and foster political instability. These attacks consume resources, diverting attention and straining the electoral infrastructure. Furthermore, DDoS attacks can serve as diversionary tactics to distract defenders from other cyberattacks targeting the election system.

148 McNamara, L., 'Framing the Problem: Cyber Threats and Elections', Mandiant, 30 May, 2019. Available at https://www.mandiant.com/resources/blog/framing-problem-cyber-threats-and-elections (accessed August 2023).

149 Van Der Staak, S., Wolf, P., *Cybersecurity in Elections: Models of Interagency Collaboration*, International Institute for Democracy and Electoral Assistance, 2019, p.16. Available at https://www.idea.int/publications/catalogue/cybersecurity-in-elections (accessed August 2023).

150 Reuters, 'Czech Election Websites Hacked, Vote Unaffected - Statistics Office', 22 October, 2017. Available at https://www.reuters.com/article/czech-election-cyber-idUSL8N1MX0OB (accessed August 2023).

### Box 9: Russian attempts to meddle in the 2021 German elections

Country(ies) affected: Germany

What happened: Ahead of the 2021 German federal elections, a DDoS attack disrupted the website of the Federal Returning Officer, responsible for overseeing elections on the federal level. As a result, the website was temporarily unavailable. Simultaneously, in the months leading up to the elections, a group known as 'Ghostwriter', linked to the Russian GRU military intelligence service, launched a hacking campaign against German federal and state MPs. The hackers sent phishing emails to steal personal login data of German lawmakers. Germany publicly attributed the illegal cyber activities of 'Ghostwriter' to Moscow. However, in November 2021, Mandiant, an American cybersecurity company and a subsidiary of Google, assessed that Belarus was at least partially responsible for the group's activity.

Why it matters: Even though it is not certain that the malicious cyber activities aimed at the 2021 German elections were coordinated, this case study shows that hostile actors may employ a combination of techniques targeting various levels of the electoral ecosystem. When added together, cyberattacks which, taken separately, have limited material impact, can have a multiplied psychological effect creating an illusion that the entire elections were rigged.

Source: Page, C., 'EU Warns Russia over "Ghostwriter" Hacking Ahead of German Elections', TechCrunch, 24 September, 2021. Available at https://techcrunch.com/2021/09/24/european-council-russia-ghostwriter/ (accessed August 2023); Mandiant, 'UNC1151 Assessed to Have Links to Belarusian Government', 16 November, 2021. Available at https://www.mandiant.com/resources/blog/unc1151-linked-to-belarus-government (accessed August 2023); The European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2022*, October 2022. Available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (accessed August 2023).

- **Website defacement**

While DDoS overwhelms a website to make it inaccessible, website defacement involves alteration of a website's appearance and content. Such attacks can be used as a means to undermine the credibility of election-related websites or to disseminate false information. This information can potentially incite voter suppression behaviour by misleading and confusing voters, for example by leading them to believe that the elections have been rescheduled or called off. Website defacement extends beyond election-related websites and can also encompass the targeting of other actors within the electoral ecosystem – political parties, candidates, government agencies, and organisations involved in election monitoring and transparency. Media outlets and social media have also been targeted by website defacement. On 6 May 2018, on the day of Latvia's general election, social network Draugiem was defaced to display a

pro-Russian message reading 'Comrades, Latvians, this concerns you. The borders of Russia have no end,' accompanied by photos of Russian soldiers in Crimea and military parades in Moscow.[151]

- **Advanced persistent threats (APTs)**

Advanced persistent threats (APTs) represent a more targeted form of attack. They involve persistent infiltration into a target's network to gather sensitive information, conduct espionage, or disrupt critical systems. APTs employ various techniques, such as social engineering, zero-day exploits (a type of attack exploiting a software's security flaw which is unknown to the vendor), and custom malware, to maintain persistence and evade detection.

Phishing, a type of social engineering, is a prevalent technique used to gain unauthorised access to personal or financial data of individuals and organisations involved, for instance, in managing and running election campaigns or infrastructure.[152] The method typically relies on fraudulent emails or messages designed to appear as if they are from trustworthy sources. Spear phishing is a more advanced form of phishing as it targets a specific individual or a number of individuals. The messages often contain enticing subject lines, official logos, and convincing language designed to mimic legitimate correspondence to gain unauthorised access to personal data. Phishing (or spear phishing) has been part of the Russian, Chinese and Iranian playbooks. In June 2020, Google's Threat Analysis Group detected phishing attempts by Iranian and Chinese APT groups targeting both Biden and Trump campaign staffers' personal emails.[153]

### 2.3.3. Targets

Malign cyber activities can be directed at various actors and levels of the electoral ecosystem.[154] The first category of targets are those involved in electoral campaigns. These include political parties, candidates and their campaign staff. Malign actors do not solely focus on the most high-profile elections. There have been numerous cases of cyber operations carried out during local elections. In July 2018, during US democratic primaries, two local democratic campaigns were hit by DDoS attacks during the active online fundraising period.[155] This example shows that a well-timed DDoS attack can hamper the political campaign's capacity to raise funds by

151 Public Broadcasting of Latvia, 'Draugiem.Lv Social Network Hacked with pro-Russia Message', 6 October, 2018. Available at https://eng.lsm.lv/article/society/crime/draugiemlv-social-network-hacked-with-pro-russia-message.a294979/ (accessed August 2023).

152 O'Connor, S., Hanson, F., Currey, E., and Beattie, T., *Cyber-Enabled Foreign Interference in Elections and Referendums*, The Australian Strategic Policy Institute, October 2020, p.10. Available at https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums (accessed August 2023).

153 Huntley, S., 'How We're Tackling Evolving Online Threats', Google Threat Analysis Group (TAG), 16 October, 2020. Available at https://blog.google/threat-analysis-group/how-were-tackling-evolving-online-threats/ (accessed August 2023).

154 McNamara, L., 'Framing the Problem: Cyber Threats and Elections', Mandiant, 30 May, 2019. Available at https://www.mandiant.com/resources/blog/framing-problem-cyber-threats-and-elections (accessed August 2023).

155 Bing, C., 'Two Democratic Campaigns Hit with DDoS Attacks in Recent Months', CyberScoop, 9 July, 2018. Available at https://cyberscoop.com/ddos-democratic-campaigns-primary-dnc-dccc/ (accessed August 2023).

disrupting online donation platforms and preventing supporters from accessing the campaign's website to contribute.

Hacking operations are not limited to the campaigns themselves but can target a vast range of organisations and entities which either provide a campaigning platform such as media outlets and social media but also entities that act as consultants or idea hubs for the candidates, such as policy advisers and think tanks. For example, Microsoft's Threat Intelligence Center (MSTIC) observed that between September 2019 and September 2020, cyber activity groups operating from Russia attacked more than 200 organisations including political campaigns, advocacy groups, parties and political consultants including US-based consultants serving Republicans and Democrats and think tanks such as the German Marshall Fund of the United States, the Aspen Institute in Germany, and the German Council on Foreign Relations (DGAP).[156]

Political institutions have also been a regular target of cyberattacks. In 2015, Germany's Bundestag was hit by a sustained cyberattack which infected a network of more than 5 600 computers and 12 000 registered users. It is estimated that the group stole a total of 16 gigabytes of data. According to German intelligence, the Russian APT28 group, linked to the GRU, was behind the attack.[157] Similarly, three months before the 2019 Australian elections, a cyberattack attributed to China's Ministry of State Security was carried out against the computer networks of Parliament and the three main political parties.[158]

Support infrastructure of the elections such as voter registers, electoral commissions and electoral boards, which support, administer and publish the results of the elections, represent another category of targets. According to Mandiant, both Chinese and Russian cyber espionage operations have targeted election administrators since 2014.[159] For example, in March 2019, Indonesia's national election commission reported that Chinese and Russian hackers probed the Indonesia voter database ahead of presidential and legislative elections in the country.[160]

156 Burt, T., 'New Steps to Protect Europe from Continued Cyber Threats', Microsoft, February 20, 2019. Available at https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/ (accessed August 2023).

157 Stelzenmüller, C., 'The Impact of Russian Interference on Germany's 2017 Elections', Brookings Institution, 28 June, 2017. Available at https://www.brookings.edu/articles/the-impact-of-russian-interference-on-germanys-2017-elections/ (accessed August 2023).

158 Reuters, 'Exclusive: Australia Concluded China Was behind Hack on Parliament, Political Parties – Sources', 15 September, 2019. Available at https://www.reuters.com/article/us-australia-china-cyber-exclusive-idUSKBN1W00VF (accessed August 2023).

159 Lim, Y., 'Election Cyber Threats in the Asia-Pacific Region', Mandiant, 22 November, 2020. Available at https://www.mandiant.com/resources/blog/election-cyber-threats-in-the-asia-pacific-region (accessed August 2023).

160 Lamb, K., 'Indonesia Election Mired in Claims of Foreign Hacking and 'Ghost' Voters', The Guardian, 19 March, 2019. Available at https://www.theguardian.com/world/2019/mar/19/indonesia-election-mired-in-claims-of-foreign-hacking-and-ghost-voters (accessed August 2023).

Similarly, in the run-up to the 2018 Colombian elections, cyberattacks against the voter registration system were launched from Venezuela, Russia's key ally in the region.[161]

Attacks aimed directly at the core electoral infrastructure including vote tabulation systems or voting machines present the greatest risk as such operations have the potential to disrupt voting, change votes or disrupt the ability to transmit election results in a timely manner. However, there is limited evidence of intrusion activity targeting core election infrastructure.[162] According to a Joint report of the US Department of Justice and the Department of Homeland Security, in 2020, Russian and Iranian campaigns did compromise 'the security of several networks that managed some election functions', however, the operation is believed not to have affected the integrity of the voting process.[163]

### 2.3.4. Perpetrators

Russia, Iran, China and North Korea are leading state actors in the field of malicious cyber activity. While Russia's primary goal is to sow divisions in Western society, China has traditionally focused on espionage, more specifically on intellectual property theft, and Iran and North Korea mostly engage in cybercrimes.[164] Nonetheless, they have all been involved in election-related cyber activities and most of the election interference incidents in the realm of cyber activity were attributed to this so-called Big Four.[165] Russia remains the most prominent state actor engaging in cyber threat activity. However, many experts believe that in the long term, cyber threats originating from China may pose greater risks.[166]

Russia conducts a whole spectrum of operations, however, its track record of cyber activity is indicative of its inclination towards 'hack and leak' operations, an approach combining

161 Arostegui, M., 'Colombia Probes Voter Registration Cyberattacks Traced to Russia's Allies', Voice of America (VOA), 15 March, 2018. Available at https://www.voanews.com/a/colombia-voter-registration-cyberattacks-russia-allies/4300571.html (accessed August 2023).

162 McNamara, L., 'Framing the Problem: Cyber Threats and Elections', Mandiant, 30 May, 2019. Available at https://www.mandiant.com/resources/blog/framing-problem-cyber-threats-and-elections (accessed August 2023).

163 Homeland Security, 'Key Findings and Recommendations from the Joint Report of the Department of Justice and the Department of Homeland Security on Foreign Interference Targeting Election Infrastructure or Political Organization, Campaign, or Candidate Infrastructure Related to the 2020 US Federal Elections', March 2021. Available at https://www.dhs.gov/publication/key-findings-and-recommendations-foreign-interference-related-2020-us-federal-elections (accessed August 2023).

164 Youtube, 'Ran Shahor Cyber Week 2022', 2022. Available at https://www.youtube.com/watch?v=CC9meMEesAk (accessed August 2023).

165 O'Connor, S., Hanson, F., Currey, E., and Beattie, T., *Cyber-Enabled Foreign Interference in Elections and Referendums*, The Australian Strategic Policy Institute, October 2020, pp.13. Available at https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums (accessed August 2023).

166 Alspach, K., 'Russian Hackers Get the Headlines. But China Is the Bigger Threat to Many US Enterprises.', Protocol, 3 August, 2022. Available at https://www.protocol.com/enterprise/china-hacking-ip-russia-cybersecurity (accessed August 2023).

cyberattacks and information campaigns.[167] Russia has replicated this method in the Syria conflict, during the European Union refugee and the 2015 migrant crisis and in the 2016 US Presidential election.[168] Based on the above mentioned reports, the pattern seems to be as follows: A Russian sponsored group (usually APT28) compromises the internal systems of a victim organisation, steals personal or financial data and then proceeds to leak it to advance Russia's political objectives. As we can see in the case of Russian meddling into the 2017 French Presidential election, also known as the 'Macron leaks,' the content can then be further amplified by Russia's proxy media outlets or by using bots and special hashtags such as #MacronLeaks.[169] It is also worth noting that the timing of the release of the documents can be of particular importance in a given operation. Macron's campaign was hacked as early as October 2016. Yet, the hackers waited to release the stolen documents until the very last moment before the media silence period which prohibits candidates from making statements or interviews in the forty-four hours before the polls close.[170]

The UK authorities believe that Russia attempted to interfere with the 2019 general election by stealing and leaking documents connected to the Free Trade Agreement between the United Kingdom and the United States. More recently, in November 2022, Russia-backed hackers stole and published Telegram conversations of Moldova's Minister of Justice, Sergiu Litvinenco, and the President's security adviser, Dorin Recean.[171]

Russia's intent is to sow chaos and divisions within Western societies. This is well shown by the example of Russian attempts to interfere with the 2017 snap elections in the United Kingdom. During the three months before the elections, the UK's National Cyber Security Center (NCSC) detected at least 188 cyberattacks by Russian and Chinese state-sponsored hackers.[172] As Thomas Rid, professor of strategic studies at Johns Hopkins University's School of Advanced International Studies, explains, in the aftermath of the Brexit vote, Russia had no motivation to

167 Tennis, M., 'Russia Ramps up Global Elections Interference: Lessons for the United States', Center for Strategic and International Studies (CSIS), 20 July, 2020. Available at https://www.csis.org/blogs/strategic-technologies-blog/russia-ramps-global-elections-interference-lessons-united-states (accessed August 2023).

168 FireEye, *APT28: At the Center of the Storm*, January 2017, p. 2. Available at https://www.mandiant.com/resources/reports/apt28-center-storm (accessed August 2023).

169 Brattberg, E., Maurer, T., Five European Experiences with Russian Election Interference, Carnegie Endowment for International Peace, 2018. Available at https://www.jstor.org/stable/resrep21009.6 (accessed August 2023).

170 Jeangène Vilmer, J.B., *The 'Macron Leaks'Operation: A Post-Mortem*, Atlantic Council Policy, June 2019, p. 19. Available at https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf (accessed August 2023).

171 Newman, L.H., 'Security News This Week: A Destabilizing Hack-and-Leak Operation Hits Moldova', Wired, 19 October, 2022. Available at https://www.wired.com/story/moldova-leaks-google-privacy-settlement-world-cup-apps/ (accessed August 2023).

172 BBC News, 'UK Targeted by "dozens" of Serious Cyber Attacks Each Month', 12 February, 2017. Available at https://www.bbc.com/news/uk-38951172 (accessed August 2023).

meddle in favour of one particular candidate but rather to 'sow distrust in democracy' within the already divided society.[173]

Russian malicious cyber activity is characterised by risky and bold behaviour and its operations are supposed to create noise and chaos.[174] In that vein, Russian hackers display a lack of concern for being apprehended. Referring to the hacking of DNC networks, the spokesman of Fire Eye, a prominent cybersecurity company, said that [Fancy Bear and Cozy Bear, nicknames frequently used for APT28 and 29] 'wanted experts and policymakers to know that Russia is behind it.'[175] Publication of its cyber operations can thus be part of Russia's strategy to undermine public trust in electoral or other democratic processes.

Hacking groups linked to Russia's intelligence services have been on Europe's radar since well before the 2016 US election hacking. As early as 2014, Russia launched a cyberattack against the Polish electoral commission's website undermining the credibility of the vote.[176] The same year, the network of the Ukrainian Central Election Commission fell victim to defacement and exploitation by Russian military hackers, an incident that is widely regarded as a precursor to the Kremlin's subsequent interference in the 2016 US election.[177] Furthermore, the Dutch intelligence agency AIVD monitored the activity of the Cozy Bear group, also known as APT29, which is thought to be associated with Russia's FSB or SVR and was one of the groups involved in the hacking of the US Democratic Party's and US government servers.[178] The Dutch agency provided the FBI with key pieces of intelligence on Russia's electoral interference. In another incident, Russia attempted to hack e-mail accounts of Dutch government employees ahead of the 2017 elections.[179] Germany also has extensive experience with Russia's cyber interference. Ahead of the 2015 federal elections, the computer system of the German Bundestag fell victim to a cyber

173 Brattberg, E., Maurer, T., Five European Experiences with Russian Election Interference, Carnegie Endowment for International Peace, 2018, p.14. Available at https://www.jstor.org/stable/resrep21009.6 (accessed August 2023).

174 Marks, J., 'Is Russia or China the Biggest Cyber Threat? Experts Are Split', Washington Post, 20 January, 2022. Available at https://www.washingtonpost.com/politics/2022/01/20/is-russia-or-china-biggest-cyber-threat-experts-are-split/ (accessed August 2023).

175 Ravindranath, M., 'Russia Wanted to Be Caught, Says Company Waging War on the DNC Hackers - Defense One', Defense One, 27 July, 2016. Available at https://www.defenseone.com/technology/2016/07/Russia-wanted-to-be-caught/130312/ (accessed August 2023).

176 AP News, 'Polish Election Commission Website Hacked', 19 November, 2014. Available at https://apnews.com/article/-----5aba677736f6448ab0a33740bb057499 (accessed August 2023).

177 The Atlantic Council, 'Foreign Interference in Ukraine's Democracy', 15 May, 2019. Available at https://www.atlanticcouncil.org/in-depth-research-reports/report/foreign-interference-in-ukraine-s-election/ (accessed Auguste 2023).

178 Paganini, P., 'The Dutch Intelligence Service AIVD "Hacked" Russian Cozy Bear Systems for Years', Security Affairs, 26 January, 2018. Available at https://securityaffairs.com/68241/intelligence/aivd-hacked-cozy-bear.html (accessed August 2023).

179 Lageman, T., 'Russian Hackers and the Dutch Election', Deutsche Welle, 3 October, 2017. Available at https://www.dw.com/en/russian-hackers-use-dutch-polls-as-practice/a-37850898 (accessed August 2023).

assault attributed to Russia,[180] carried out with the intention of gathering intelligence that could be used as part of a disinformation campaign or for influence operations.[181] The group, also known as Pawn Storm or Fancy Bear, a group responsible for both the 2016 US Election hacking and the Macron leaks, was also attempting to steal e-mail credentials from members of the Christian Democratic Union of Germany (CDU).[182]

In the past few years, Russia has emerged as the most prominent foreign actor engaging in hostile cyber activity in Europe. In the months leading up to the last EU parliamentary elections, Fire Eye observed an increase in cyberattacks against European government departments and agencies as well as media outlets in Germany and France.[183] We can thus conclude that Russia is likely to remain a credible threat for the upcoming elections.

Compared to Russia, China has so far not shown much inclination towards hacking for the purpose of leaking candidate secrets.[184] On the other hand, it has a well-documented history of cyber espionage operations.[185] It is particularly concerning that these operations are designed to collect information, therefore their objective is to avoid being caught. In the past, Chinese APT groups targeting critical systems remained undetected for a decade.[186] China's large-scale phishing and hacking campaign in Cambodia provides an insight into China's operating procedure. Ahead of Cambodia's 2018 elections, a Chinese group known as TEMP.Periscope compromised a wide range of targets involved in the electoral process including the national election commission, several ministries, the Cambodian Senate, an opposition MP, human rights and democracy advocates, two Cambodian diplomats serving overseas and a multitude of

180 Deutsche Welle, 'Bundestag IT System Shut Down', 20 August, 2015. Available at https://www.dw.com/en/bundestag-it-system-shut-down-after-hacker-attack/a-18659654 (accessed August 2023).

181 Committee on Foreign Relations, US Senate, 'Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for US National Security', A Minority Staff Report, 10 January, 2018. Available at https://www.govinfo.gov/app/details/CPRT-115SPRT28110/CPRT-115SPRT28110/summary (accessed August 2023).

182 Auchard, E., 'Hackers Try to Attack Merkel's Party, Security Consultants Say', Reuters, 11 May, 2016. Available at https://www.reuters.com/article/us-germany-cyber-security-idUSKCN0Y22KV (accessed August 2023).

183 O'Sullivan, D., 'Russian Hackers Targeting European Governments before Elections, Security Firm Warns', CNN, 22 March, 2019. Available at https://www.cnn.com/2019/03/22/europe/russia-hackers-european-elections-intl/index.html (accessed August 2023).

184 O'Sullivan, D., 'Russian Hackers Targeting European Governments before Elections, Security Firm Warns', CNN, 22 March, 2019. Available at https://www.cnn.com/2019/03/22/europe/russia-hackers-european-elections-intl/index.html (accessed August 2023).

185 Alspach, K., 'Russian Hackers Get the Headlines. But China Is the Bigger Threat to Many US Enterprises.', Protocol, 3 August, 2022. Available at https://www.protocol.com/enterprise/china-hacking-ip-russia-cybersecurity (accessed August 2023).

186 Winder, D., 'Linux Security: Chinese State Hackers May Have Compromised "Holy Grail" Targets Since 2012', Forbes, 7 April, 2020. Available at https://www.forbes.com/sites/daveywinder/2020/04/07/linux-security-chinese-state-hackers-have-compromised-holy-grail-targets-since-2012/ (accessed August 2023).

Cambodian media entities.[187] The purpose of the operation remains unclear. According to Mandiant, an American cybersecurity company and a subsidiary of Google, election monitoring could have been the rationale behind the operation.[188] Possible destabilisation of Cambodia's domestic situation could threaten China's interests as Cambodia is one of Beijing's key allies in the region. It is thus possible that China engaged in intelligence gathering to monitor political developments in the country and detect early signs of a potential political change. However, it cannot be ruled out that the intrusion was part of a larger operation.[189]

In recent years, experts have noted an upward trend in incidents of China's foreign interference.[190] Although China does not necessarily engage in the most technically advanced attacks, the size of its talent pool, the resources it directs towards the operations and its persistence should be a source of concern.[191] Over time, China is perfecting its techniques. According to CrowdStrike, in 2021, 'China-nexus actors emerged as the leader in vulnerability exploitation.'[192] Even though China has mostly engaged in election-related cyber activity in the Asia-Pacific region where it was involved in 20 campaigns mostly targeting Hong Kong and Taiwan, it is possible that China will mimic TTPs elsewhere in the world.[193] With China's increasing global ambitions and the changing geopolitical landscape in the context of the increasing rivalry between the US and China and the recalibration of EU policy on China, Beijing's stakes in the European elections are getting higher.

187 Henderson, S., Miller, S., Perez, D., Siedlarz, M., Wilson, B., Read, B., 'Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally', Mandiant, 10 July, 2018. Available at https://www.mandiant.com/resources/blog/chinese-espionage-group-targets-cambodia-ahead-of-elections (accessed August 2023).

188 Henderson, S., Miller, S., Perez, D., Siedlarz, M., Wilson, B., Read, B., 'Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally', Mandiant, 10 July, 2018. Available at https://www.mandiant.com/resources/blog/chinese-espionage-group-targets-cambodia-ahead-of-elections (accessed August 2023).

189 Henderson, S., Miller, S., Perez, D., Siedlarz, M., Wilson, B., Read, B., 'Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally', Mandiant, 10 July, 2018. Available at https://www.mandiant.com/resources/blog/chinese-espionage-group-targets-cambodia-ahead-of-elections (accessed August 2023).

190 O'Connor, S., Hanson, F., Currey, E., and Beattie, T., *Cyber-Enabled Foreign Interference in Elections and Referendums*, The Australian Strategic Policy Institute, October 2020, pp. 31-45. Available at https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums (accessed August 2023).

191 Alspach, K., 'Russian Hackers Get the Headlines. But China Is the Bigger Threat to Many US Enterprises.', Protocol, 3 August, 2022. Available at https://www.protocol.com/enterprise/china-hacking-ip-russia-cybersecurity (accessed August 2023).

192 CrowdStrike, *CrowdStrike 2023 Global Threat Report*, February 2022. Available at https://www.crowdstrike.com/press-releases/crowdstrikes-annual-threat-report-exposes-evolution-of-ecrime-ecosystem/ (accessed August 2023).

193 Lim, Y., 'Election Cyber Threats in the Asia-Pacific Region', Mandiant, 22 November, 2020. Available at https://www.mandiant.com/resources/blog/election-cyber-threats-in-the-asia-pacific-region (accessed August 2023).

Furthermore, it has a documented history of cyber operations in Europe, including the targeting of European diplomatic corps. In the past, European institutions have suffered from cyberattacks perpetrated by China-backed hacking groups. Last year, Google's Threat Analysis Group (TAG) detected phishing attempts by a Chinese hacking group called Mustang Panda targeting European entities. The e-mails contained malicious attached files with names such as 'Situation at the EU borders with Ukraine.zip.' According to TAG: 'Targeting of European organisations has represented a shift from Mustang Panda's regularly observed Southeast Asian targets.'[194]

Compared to Russian operations which are designed to create noise, China's attacks are meant to happen undercover.[195] It is thus possible that a number of Chinese attacks have gone undetected, preventing cybersecurity experts or policymakers from drawing the whole picture of China's malicious cyber activities.

### 2.3.5. Reflection

Even though Russia remains the number one cyber threat to the European democratic processes, both Russia and China represent credible cyber risks to the integrity of the 2024 European parliamentary elections. The recent history of their cyber activities on the continent shows that they both have capabilities and motivations to interfere through cyber tools in the electoral process. China-based threat actors have optimised and sophisticated their operations.[196] They have become leaders in discovering and developing zero-day exploits.[197] This could be linked to a Chinese regulation which entered into effect in September 2021 imposing the obligation on vendors to report zero-day vulnerabilities to the government.[198]

The conflict in Ukraine transformed the cyber threat landscape giving rise to cyberattacks against Ukraine but also targeting governmental organisations across Europe which have provided assistance to Ukraine, in particular countries bordering Ukraine and NATO allies.[199] DDoS attacks

194 Brewster, T. , 'Chinese Hackers Launch Attacks On European Officials In Russia-Ukraine War', Forbes, 8 March, 2022. Available at https://www.forbes.com/sites/thomasbrewster/2022/03/08/chinese-hackers-ramp-up-europe-attacks-in-time-with-russia-ukraine-war/ (accessed August 2023).

195 Alspach, K., 'Russian Hackers Get the Headlines. But China Is the Bigger Threat to Many US Enterprises', Protocol, 3 August, 2022. Available at https://www.protocol.com/enterprise/china-hacking-ip-russia-cybersecurity (accessed August 2023).

196 PwC, *Cyber Threats 2022: A Year in Retrospect,* 2023, p. 20. Available at https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html (accessed August 2023).

197 Microsoft, Microsoft Digital Defense Report 2022, 2022. Available at https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022 (accessed August 2023).

198 Microsoft, Microsoft Digital Defense Report 2022, 2022. Available at https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022 (accessed August 2023).

199 Smith, B., 'Defending Ukraine: Early Lessons from the Cyber War', Microsoft, 22 June, 2022. Available at https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/ (accessed August 2023).

have been launched against Baltic states, Poland and other allies of Ukraine.[200] The European Union Agency for Cybersecurity (ENISA) assesses that we will continue to see disruptive operations by nation state threat actors in the context of the war.[201] Russia might become even bolder in its hostile cyber activity as it has little to lose in the current geopolitical situation. China, on the other hand, is likely to stick to covert operations. With the increasing geopolitical rivalry between the US and China, Beijing might be even more interested in steering the EU's policy-making in its favour. Based on China's pattern of behaviour across Asia-Pacific, China could engage in election-related cyber espionage during European elections to gather intelligence on policy stances of political candidates and political parties.

In recent months, experts have witnessed a rise in DDoS attacks as well as incidents using social engineering techniques such as phishing.[202] This trend will likely continue in the months leading up to the European 2024 parliamentary elections. Similarly to the previous elections, we might see a wave of cyberattacks directed at government entities and media outlets.

Since the last elections, European institutions as well as national governments are better protected against cyber threats. In the changing geopolitical context, cyber security has become a priority for governments.[203] The European Union has also taken steps to boost the bloc's cyber resilience.[204] In 2019, the EU's Cyber Diplomacy Toolbox was set up allowing member states to collectively respond to cyber incidents. In 2020, the EU launched a new cyber security strategy. Increased defence cooperation within the framework of the Permanent Structured Cooperation (PESCO) led to the establishment of Cyber Rapid Response Teams (CRRTs). Together, these instruments have contributed to increasing the EU's capacities to tackle cyber threats. However, remaining challenges include the scarcity of manpower trained in cyber security as well as the low awareness of cyber threats among political parties and candidates. According to ENISA's analysis, the political campaigning process is the most susceptible to cyber security risks in the

200 State Security Department of the Republic of Lithuania and Defence Intelligence and Security Service under the Ministry of National Defence, 'National Threat Assessment 2023'. Available at https://kam.lt/wp-content/uploads/2023/03/Assessment-of-Threats-to-National-Security-2022-published-2023.pdf (accessed August 2023).

201 The European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2022*, October 2022. Available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (accessed August 2023).

202 The European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2022*, October 2022. Available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (accessed August 2023).

203 Pennings, F., 'Cyber Resilience Act: A Step towards Safe and Secure Digital Products in Europe', Microsoft, 16 February, 2023. Available at https://blogs.microsoft.com/eupolicy/2023/02/16/cyber-resilience-act-cybersecurity-skills/ (accessed August 2023).

204 European Parliamentary Research Service, 'Future Shocks 2022: Building a Healthier Online Environment for Healthy Democracies', 19 May, 2022. Available at https://epthinktank.eu/2022/05/19/future-shocks-2022-building-a-healthier-online-environment-for-healthy-democracies/ (accessed August 2023).

election lifecycle.[205] Political candidates and their staffers can easily fall victim to social engineering techniques and expose their campaigns to the risk of the 'hack and leak' scenario.

205 The European Union Agency for Cybersecurity (ENISA), *Election Cybersecurity: Challenges and Opportunities*, February 2019. Available at https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/election-cybersecurity-challenges-and-opportunities (accessed August 2023).

# 3. CONCLUSION

Europe has not escaped from attempts of external interference in its elections, as evidenced by the multiple cases expounded upon in this study. Additionally, the attractiveness of election interference as a relatively low-cost, high-impact method of interference ensures their continued use by malign foreign state and state-linked actors. Given this context, it is unreasonable to assume that the upcoming 2024 European elections will remain immune to attempts of election interference. While acknowledging the persistent threats, it's essential to recognize that there are safeguards in place to counter external interference in European elections, including enhanced information campaigns, election monitoring, and collaborative efforts with tech companies to detect and mitigate disinformation and cyberattacks.

The general aim of the interveners is to instil doubt and suspicion regarding the integrity of electoral systems and foster instability and division within societies. The European Parliament election is potentially susceptible in this context as it is composed of 27 elections spread across Europe. Early indicators have already emerged, such as a surge in DDoS attacks and incidents using social engineering tactics like phishing across Europe, bolstering the hypothesis that the European elections are attractive targets for malign foreign state and non-state actors. This is further compounded by the ongoing support extended to Ukraine by EU and NATO countries, effectively elevating Europe's profile as a focal point for certain international actors.

As demonstrated by the study, electoral interventions manifest in diverse forms, often interconnected in practice. However, while more methods exist for election interventions, the authors selectively examined those they assess as the most plausible within the European election context. These methods include financial avenues such as the funding of political parties, politicians, and campaigns, as well as engaging in vote buying, incentivising voters, and leveraging diasporas on behalf of third countries. These direct approaches may be accompanied by orchestrated information manipulation campaigns conducted by malign foreign state and state-affiliated actors. Tactics include disseminating disinformation, employing typosquatting, and resorting to intimidation tactics against critical voices (including SLAPPs). Furthermore, malign foreign actors might even influence the voting process itself through 'hack and leak' campaigns, DDoS attacks, or compromising electoral infrastructure. It is crucial to recognise that the tactics employed for interference are not fixed – they undergo evolution over time, as malign actors derive inspiration from one another.

However, among these domains, the authors highlight financial instruments as particularly worrisome, whilst information manipulation assumes a central role in fomenting heightened social tensions and nurturing the seeds of public mistrust. In contrast, the feasibility of solely altering election outcomes through cyber operations remains doubtful. Moreover, the nature of these non-financial tactics inherently lends itself to plausible deniability. This characteristic contrasts with financial incentives, which frequently involve the recipient's knowledge and active participation in accepting the loan, donation or other financial or in-kind benefit.

It is important to highlight that officials from various countries often refrain from disclosing explicit details regarding the methods employed by malign foreign actors in electoral interventions. The study thus relied on open-source material. Quite often the details of operations

are obfuscated, and national authorities acknowledge only the existence of such attempts. Thus, cases of electoral interventions may well be more widespread.

In most major cases of information manipulation done by malign state and non-state actors and reported in Europe, initial information has surfaced from investigative NGOs, journalists, or academics. Only subsequently have the national governments initiated inquiries. It could also be suggested that, in certain scenarios, individuals privy to sensitive information, including government figures, may lack the authorisation to divulge their data or sources. As a result, they might strategically initiate targeted leaks, prompting the civil sector to disseminate the information instead.

The study revealed that both Russia and China have been active participants in election interventions across all three analysed dimensions. Given this pattern, the authors hold the view that it is probable that these two actors may engage in interventions during the 2024 European elections. In particular, Russia's historical involvement in electoral interventions in Europe is noteworthy, driven by the goal of sowing discord and undermining transatlantic unity. In contrast, China's engagement in European affairs is a relatively recent development, and its primary intervention focus has thus far been concentrated in the Asia-Pacific region.

In the short term, the more immediate threat may be posed by Russia, which has effectively harnessed financial incentives, information manipulation as well as cyber tools to intervene in elections. This capability has positioned Russia as a significant challenge, using sophisticated methods to manipulate elections for strategic gains. Comparatively, while China's engagement in (chiefly) information manipulation within Western contexts has been growing, its endeavours have not reached the breadth, complexity, and impact of the Russian campaigns.

When it comes to leveraging financial incentives, Russia has demonstrated a more pronounced tendency to provide direct financial and in-kind support to political parties, candidates, and campaigns across Europe. In contrast, China's approach in Europe has centred around geoeconomics, focusing on the promotion of initiatives like the Belt and Road initiative and its cooperative framework with Central and Eastern Europe (previously known as the 16+1 platform). China often employs a combination of rewards and punitive measures in its interactions with political representatives from various countries. Noteworthy is China's strategic outreach for political influence, which frequently extends not only to national officials but also encompasses those at the provincial and municipal levels. This aspect accentuates the significance of these less-studied and regulated tiers within the electoral intervention landscape.

The attempts of exploitation of diasporic communities as a means of election intervention has been a notable aspect of China's strategy in countries of Asia-Pacific, most notably in Australia and Canada. However, this tactic has been less conspicuous within the European context. Conversely, Russia has displayed a relatively restrained utilisation of this approach.

In the sphere of information manipulation campaigns centred around elections, Russia's foremost goal is to sow discord, in accordance with its view of the current information landscape as an arena of active battleground with the West. This perspective frames the situation as an armed struggle that Russia must emerge victorious from. On the contrary, the aim of the actors linked to China in information manipulation campaigns has predominantly been to present China's

authoritarian government in a favourable light. China's campaigns have aimed to position China as a viable governance model, suppress criticism, and garner vocal support from foreign policymakers.

The distinctions between Russia and China become even more evident when studying disinformation campaigns. Russia-backed disinformation operations actively aim to influence the political landscape, sway public opinions, erode trust in democratic processes, and fuel divisive sentiments. Russia's approach seeks to confound rather than convince. In contrast, China places a significant emphasis on discursive power, and within the European information space, a burgeoning network of Chinese state-affiliated actors work to amplify disinformation. In essence, China's current approach to disinformation in Europe still leans more toward coercing rather than confounding.

This does not, however, mean that China's tactics are less harmful. Apart from portraying China in a positive light, its disinformation strategy in Europe also aims to tarnish the US' reputation and create division within the transatlantic partnership. To achieve these goals, Chinese state-affiliated entities have aligned themselves with Russian disinformation efforts, sometimes even endorsing assertions like the existence of 'US biolabs in Ukraine'. In specific instances, China-originated disinformation serves both of its objectives, such as the contention that COVID-19 originated in the US rather than China.

Unlike Russia, China has not yet assumed the role of a major player in utilising disinformation as a weapon during European elections. Nevertheless, a convergence of factors, including Beijing's interest in undermining the US-EU relationship and its track record of amplifying Russian disinformation, endows China with the capacity to evolve into a noteworthy concern over time.

In the realm of cyber-enabled election interventions, Russia poses a more immediate threat compared to other state actors. However, China emerges as a formidable contender with enduring potential. While Russia has primarily concentrated on election interventions, China has historically prioritised espionage, particularly intellectual property theft, whereas Iran and North Korea have predominantly engaged in cybercriminal activities. Despite these varied focuses, all four nations have been implicated in election-related cyber operations, earning them the collective label of the 'Big Four' in this arena.

Russian malicious cyber activities, including those aimed at election interventions, are characterised by audacious and high-risk behaviour, aiming to generate disruption and chaos. Russian hackers exhibit a brazen disregard for the possibility of apprehension. In contrast, China's operations are meticulously designed for information gathering, with a paramount emphasis on avoiding detection. Some Chinese Advanced Persistent Threat (APT) groups have operated undetected for a decade while targeting critical systems. Although China may not consistently execute the most technologically advanced attacks, the extensive talent pool, substantial resource allocation, and unwavering persistence magnify its significance as a potential threat.

In conclusion, the spectrum of electoral interventions encompasses diverse methods, ranging from rudimentary to technologically advanced, rendering many avenues accessible to a wide array of malign foreign state and non-state actors. The intricate issue of attribution complicates matters, given the complexity and sensitivity surrounding identifying the culprits. The adeptness

of these actors in concealing their origins compounds the challenge, particularly in cyber-enabled election interventions where false flag operations are frequently employed to obfuscate true authorship.

A different sort of challenge lies in the realm of information manipulation where the line between free speech and spreading misinformation and disinformation may be thin. While legislative measures can act as an initial layer of defence for the European landscape surrounding elections, their efficacy hinges on a collaborative effort encompassing society as a whole. A solution lies in further enhancing the transparency and resilience of election processes within the European Union. Simultaneously, increasing the costs for those who seek to intervene could deter their efforts. Ultimately, safeguarding the integrity of European elections necessitates a multifaceted strategy that engages all sectors of society.

# REFERENCES


- '18 May Yevgeniy Prigozhin's SLAPP Action against Bellingcat Founder Is Struck out' [Press release], McCue Jury & Partners, 18 May, 2022. Available at https://www.mccue-law.com/yevgeniy-prigozhins-action-against-bellingcat-founder-struck-out/ (accessed August 2023).
- Akinlolu, A., Ogunnubi, O., 'Russo-African Relations and Electoral Democracy: Assessing the Implications of Russia's Renewed Interest for Africa', *African Security Review*, Vol. 30, No. 3, July 3, 2021, p. 387.
- Alaphilippe, A., Machado, G., Miguel, R., Poldi, F., 'Doppelganger - Media Clones Serving Russian Propaganda', EU DisinfoLab, 27 September, 2022. Available at https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf (accessed August 2023).
- Alizadeh, M., Shapiro, J.N., Buntain, C., Tucker, J.A., 'Content-Based Features Predict Social Media Influence Operations', *Science Advances*, Vol. 6, No. 30, 24 July, 2020.
- Alliance Canada Hong Kong, 'In Plain Sight: Beijing's Unrestricted Network of Foreign Influence in Canada', May 2021. Available at https://alliancecanadahk.com/wp-content/uploads/2022/06/ACHK_InPlainSight.pdf (accessed August 2023).
- Alliance for Securing Democracy - German Marshall Fund, 'Authoritarian Interference Tracker'. Available at https://securingdemocracy.gmfus.org/toolbox/authoritarian-interference-tracker/ (accessed August 2023).
- Allina-Pisano, J., 'Social Contracts and Authoritarian Projects in Post-Soviet Space: The Use of Administrative Resource', *Communist and Post-Communist Studies*, Vol. 43, No. 4, December 1, 2010, pp. 373–382.
- Alspach, K., 'Russian Hackers Get the Headlines. But China Is the Bigger Threat to Many US Enterprises.', Protocol, 3 August, 2022. Available at https://www.protocol.com/enterprise/china-hacking-ip-russia-cybersecurity (accessed August 2023).
- AP News, 'Polish Election Commission Website Hacked', 19 November, 2014. Available at https://apnews.com/article/-----5aba677736f6448ab0a33740bb057499 (accessed August 2023).
- Armstrong, S., 'Learning the Right Lessons from Chinese Sanctions on Australian Imports', East Asia Forum, 16 April, 2023. Available at https://www.eastasiaforum.org/2023/04/16/learning-the-right-lessons-from-chinese-sanctions-on-australian-imports/ (accessed August 2023).
- Arostegui, M., 'Colombia Probes Voter Registration Cyberattacks Traced to Russia's Allies', Voice of America (VOA), 15 March, 2018. Available at https://www.voanews.com/a/colombia-voter-registration-cyberattacks-russia-allies/4300571.html (accessed August 2023).

- Auchard, E., 'Hackers Try to Attack Merkel's Party, Security Consultants Say', Reuters, 11 May, 2016. Available at https://www.reuters.com/article/us-germany-cyber-security-idUSKCN0Y22KV (accessed August 2023).
- Balding, C., Potter, R., et al., 'Chinese Open Source Data Collection, Big Data, And Private Enterprise Work For State Intelligence and Security: The Case of Shenzhen Zhenhua', Rochester, NY, 13 September, 2020. Available at https://ssrn.com/abstract=3691999 (accessed August 2023).
- Baquero, A., Hall, K.G., Tsogoeva, A., Albalat, J. G., Grozev, C., Bagnoli, L., Vergine, S., 'Fueling Secession, Promising Bitcoins: How a Russian Operator Urged Catalonian Leaders to Break with Madrid', Organized Crime and Corruption Reporting Project, 8 May, 2022. Available at https://www.occrp.org/en/investigations/fueling-secession-promising-bitcoins-how-a-russian-operator-urged-catalonian-leaders-to-break-with-madrid (accessed August 2023).
- Barros, B., Soula, E., 'Here and Now: Chinese Interference in the Transatlantic Space', Alliance for Securing Democracy - German Marshall Fund, 9 February, 2021. Available at https://securingdemocracy.gmfus.org/here-and-now-chinese-interference-in-the-transatlantic-space/ (accessed August 2023).
- BBC News, 'Turkey's Erdogan Says German Leaders Are Enemies', 18 August, 2017. Available at https://www.bbc.com/news/world-europe-40973197 (accessed August 2023).
- BBC News, 'UK Targeted by "dozens" of Serious Cyber Attacks Each Month', 12 February, 2017. Available at https://www.bbc.com/news/uk-38951172 (accessed August 2023).
- Belton, C., Harris, S., Mekhennet, S., 'Kremlin Tries to Build Antiwar Coalition in Germany, Documents Show', Washington Post, 21 April, 2023. Available at https://www.washingtonpost.com/world/2023/04/21/germany-russia-interference-afd-wagenknecht/ (accessed August 2023).
- Benkler, Y., Faris, R., Roberts, H., *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*, Oxford University Press, New York, 2018, p. 147.
- Bennett, W. L., Livingston, S. eds., *The Disinformation Age: Politics, Technology, and Disruptive Communication in the United States*, 1st ed., Cambridge University Press, Cambridge, 2020. p. 171.
- Bērziņa-Čerenkova, U.A., Ferrari, E., Voo, J., 'Inflaming Transatlantic Tensions? China's Public Diplomacy Efforts to Influence EU-US Relations', in Rühlig, T. (ed.), *China's Digital Power*, Digital Power China research consortium (DPC), 2022, pp. 65–74.
- Bing, C., 'Two Democratic Campaigns Hit with DDoS Attacks in Recent Months', CyberScoop, 9 July, 2018. Available at https://cyberscoop.com/ddos-democratic-campaigns-primary-dnc-dccc/ (accessed August 2023).
- Bloomberg, 'China Is Said to Probe Chairman of Emerging Energy Star CEFC', 1 March, 2018. Available at https://www.bloomberg.com/news/articles/2018-03-01/cefc-chairman-ye-probed-by-chinese-authorities-caixin-reports (accessed August 2023).

- Bradshaw, P., 'Data Journalism', in Craig, D., Zion, L. (eds.), *Ethics for Digital Journalists: Emerging Best Practices*, Routledge, New York, 2015.
- Bradshaw, S., Howard, P.N., *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation*, Working Paper, Oxford, 2018. Available at https://demtech.oii.ox.ac.uk/research/posts/challenging-truth-and-trust-a-global-inventory-of-organized-social-media-manipulation/ (accessed August 2023).
- Brady, A.-M., 'The Data Dump That Reveals the Astonishing Breadth of Beijing's Interference Operations', Washington Post, 26 September, 2020. Available at https://www.washingtonpost.com/opinions/2020/09/26/data-dump-that-reveals-astonishing-breadth-beijings-interference-operations/ (accessed August 2023).
- Brattberg, E., Maurer, T., Five European Experiences with Russian Election Interference, Carnegie Endowment for International Peace, 2018. Available at https://www.jstor.org/stable/resrep21009.6 (accessed August 2023).
- Brennan, G., Lomasky, L., eds., 'The Logic of Electoral Choice', *Democracy and Decision*, 1st ed., Cambridge University Press, Cambridge, 1993, pp. 19–31.
- Brewster, T. , 'Chinese Hackers Launch Attacks On European Officials In Russia-Ukraine War', Forbes, 8 March, 2022. Available at https://www.forbes.com/sites/thomasbrewster/2022/03/08/chinese-hackers-ramp-up-europe-attacks-in-time-with-russia-ukraine-war/ (accessed August 2023).
- Bubeck, J., Marinov, N., *Rules and Allies: Foreign Election Interventions*, Cambridge University Press, Cambridge, 2019, p. 111.
- Buresh, D.L., 'Russian Cyber-Attacks on Estonia, Georgia, and Ukraine, Including Tactics, Techniques, Procedures, and Effects', *Journal of Advanced Forensic Sciences*, Vol. 1, No. 2, 19 August, 2021, pp. 15–26. Available at https://openaccesspub.org/advanced-forensic-sciences/article/1686 (accessed August 2023).
- Burt, T., 'New Steps to Protect Europe from Continued Cyber Threats', Microsoft, February 20, 2019. Available at https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/ (accessed August 2023).
- Canadian Centre for Cyber Security, 'Cyber Threat to Canada's Democratic Process', 28 February, 2019, p. 32. Available at https://www.cyber.gc.ca/sites/default/files/cyber/publications/cse-cyber-threat-assessment-e.pdf (accessed August 2023).
- 'Catherine Belton, Journalist and Author of 'Putin's People: How the KGB Took Back Russia and Then Took on the West'', The Foreign Policy Centre, 15 February, 2023. Available at https://fpc.org.uk/catherine-belton-journalist-and-author-of-putins-people-how-the-kgb-took-back-russia-and-then-took-on-the-west/ (accessed August 2023).
- CGTN, 'China Urges US to Disclose More Details about Biolabs in Ukraine', 8 March, 2022. Available at https://news.cgtn.com/news/2022-03-08/China-urges-U-S-to-disclose-details-about-biolabs-in-Ukraine-18eA7VpwQRG/index.html (accessed August 2023).

- Clough, A., de Avila, A., 'In Guarding Democracy, Hindsight Really Will Be 2020: The Tabletop Exercise as a Model for Securing American Elections', *Kennedy School Review*, Volume XX, 15 October, 2020. Available at https://ksr.hkspublications.org/2020/10/15/in-guarding-democracy-hindsight-really-will-be-2020-the-tabletop-exercise-as-a-model-for-securing-american-elections/ (accessed August 2023).
- Collier, K., 'Pro-China Social Media Campaign Sought to Influence US Voters, Researchers Say', NBC News, 26 October, 2022. Available at https://www.nbcnews.com/tech/security/-china-social-media-campaign-sought-influence-us-voters-researchers-sa-rcna53728 (accessed August 2023).
- Committee on Foreign Relations, US Senate, 'Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for US National Security', A Minority Staff Report, 10 January, 2018. Available at https://www.govinfo.gov/app/details/CPRT-115SPRT28110/CPRT-115SPRT28110/summary (accessed August 2023).
- Conley, H.A., Melino, M., 'Russian Malign Influence in Montenegro: The Weaponization and Exploitation of History, Religion, and Economics', Center for Strategic and International Studies (CSIS), 14 May, 2019. Available at https://www.csis.org/analysis/russian-malign-influence-montenegro-weaponization-and-exploitation-history-religion-and (accessed August 2023).
- Connolly, A., 'Trudeau Says Using Minister's WeChat Group to Fund Lawsuit against Journalist Was "Unacceptable"', Global News, 16 May, 2020. Available at https://globalnews.ca/news/6986602/joyce-murray-wechat-china-lawsuit/ (accessed August 2023).
- Cook, S., 'Countering Beijing's Media Manipulation', *Journal of Democracy*, Vol. 33, No. 1, 2022, pp. 116–130.
- Cooper, S., 'Canadian Intelligence Warned PM Trudeau That China Covertly Funded 2019 Election Candidates: Sources', Global News, 7 November, 2022. Available at https://globalnews.ca/news/9253386/canadian-intelligence-warned-pm-trudeau-that-china-covertly-funded-2019-election-candidates-sources/ (accessed August 2023).
- Cooper, S., 'Exclusive: Beijing Allegedly Tried to Run Candidate against Popular Canadian Mayor', The Bureau, 23 August, 2023. Available at https://www.thebureau.news/p/exclusive-beijing-allegedly-tried?utm_campaign=post (accessed August 2023).
- Cooper, S., 'Is China Influencing B.C. Politicians? Falun Gong Case Points That Way', Victoria Times Colonist, 16 September, 2014. Available at https://www.timescolonist.com/bc-news/is-china-influencing-bc-politicians-falun-gong-case-points-that-way-4613703 (accessed August 2023).
- Couzigou, I., 'The French Legislation Against Digital Information Manipulation in Electoral Campaigns: A Scope Limited by Freedom of Expression', *Election Law Journal*: *Rules, Politics, and Policy*, Vol. 20, No. 1, 1 March, 2021, pp. 98–115.

- CrowdStrike, *CrowdStrike 2023 Global Threat Report*, February 2022. Available at https://www.crowdstrike.com/press-releases/crowdstrikes-annual-threat-report-exposes-evolution-of-ecrime-ecosystem/ (accessed August 2023).
- Day, J., 'What Is a Smear Campaign? Can You Spot and Beat One?', Liberties.Eu, 28 March, 2023. Available at https://www.liberties.eu/en/stories/smear-campaign/44721 (accessed August 2023).
- Delerue, F., *Cyber Operations and International Law, Cambridge Studies in International and Comparative Law*, Cambridge University Press, Cambridge, 2020, p. 255.
- Deutsche Welle, 'Bundestag IT System Shut Down', 20 August, 2015. Available at https://www.dw.com/en/bundestag-it-system-shut-down-after-hacker-attack/a-18659654 (accessed August 2023).
- Deutsche Welle, 'Report: Russian Money Fueled AfD Trip', 22 May, 2018. Available at https://www.dw.com/en/report-afd-members-flight-sponsored-with-russian-money/a-43872774 (accessed August 2023).
- Dodman, B., 'Le Pen's Far Right Served as Mouthpiece for the Kremlin, Says French Parliamentary Report', France 24, 3 June, 2023. Available at https://www.france24.com/en/france/20230603-le-pen-s-far-right-served-as-mouthpiece-for-the-kremlin-says-french-parliamentary-report (accessed August 2023).
- Dorell, O., 'Alleged Russian Political Meddling Documented in 27 Countries since 2004', USA TODAY, 7 September, 2017. Available at https://www.usatoday.com/story/news/world/2017/09/07/alleged-russian-political-meddling-documented-27-countries-since-2004/619056001/ (accessed August 2023).
- Dos Santos, N., 'Investigation into Matteo Salvini's Lega Party's Possible Scheme with Russia', CNN, 11 July, 2019. Available at https://edition.cnn.com/2019/07/11/europe/investigation-league-salvini-russia-money-intl/index.html (accessed August 2023).
- Duberry, J., '"Dezinformatsiya" and Foreign Information Manipulation and Interference', Global Challenges, May 2023. Available at https://globalchallenges.ch/issue/13/dezinformatsiya-and-foreign-information-manipulation-and-interference/ (accessed August 2023).
- Dwoskin, E., Romm, T., 'Facebook Says It Shut down 32 False Pages and Profiles Engaged in Divisive Messaging Ahead of the US Midterm Elections', Washington Post, 31 July, 2018. Available at https://www.washingtonpost.com/technology/2018/07/31/facebook-says-it-has-uncovered-coordinated-disinformation-operation-ahead-midterm-elections/ (accessed August 2023)
- Ellehuus, R., 'Mind the Gaps: Russian Information Manipulation in the United Kingdom', Center for Strategic and International Studies, 31 January, 2020. Available at https://www.csis.org/analysis/mind-gaps-russian-information-manipulation-united-kingdom (accessed August 2023).

- European Commission, Directorate-General for Communications Networks, Content and Technology, *A multi-dimensional approach to disinformation – Report of the independent High level Group on fake news and online disinformation*, Publications Office, 2018. Available at https://data.europa.eu/doi/10.2759/739290 (accessed August 2023).
- European Parliament, Directorate-General for Internal Policies of the Union, Reed, Q., Jouan Stonestreet, B., Devrim, D. et al., *Financing of political structures in EU Member States – How funding is provided to national political parties, their foundations and parliamentary political groups, and how the use of funds is controlled*, European Parliament, 2021. Available at https://data.europa.eu/doi/10.2861/932651 (accessed August 2023).
- European Parliament, Special Committee on foreign interference in all democratic processes in the European Union, including disinformation (INGE 2), Report on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation (2022/2075(INI)), 15 May, 2023, p. 13. Available at https://www.europarl.europa.eu/doceo/document/A-9-2023-0187_EN.html (accessed August 2023).
- European Parliamentary Research Service, 'Future Shocks 2022: Building a Healthier Online Environment for Healthy Democracies', 19 May, 2022. Available at https://epthinktank.eu/2022/05/19/future-shocks-2022-building-a-healthier-online-environment-for-healthy-democracies/ (accessed August 2023).
- European Regulators Group for Audiovisual Media Services (ERGA), *Notions of Disinformation and Related Concepts*, ERGA, 2020, p. 62. Available at https://erga-online.eu/wp-content/uploads/2021/03/ERGA-SG2-Report-2020-Notions-of-disinformation-and-related-concepts-final.pdf (accessed August 2023).
- European Union External Action (EEAS), *1st EEAS Report on Foreign Information Manipulation and Interference Threats*, EEAS, 2023. Available at https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en (accessed August 2023).
- European Union: European Commission, Proposal for a Directive of the European Parliament and of the Council on protecting persons who engage in public participation from manifestly unfounded or abusive court proceedings, 27 April, 2022, COM(2022) 177 final. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0177 (accessed August 2023).
- EUvsDisinfo, 'Election Meddling and Pro-Kremlin Disinformation', 2019. Available at https://euvsdisinfo.eu/uploads/2019/10/PdfPackage_EUvsDISINFO_2019_EN_V2.pdf (accessed August 2023).
- FireEye, *APT28: At the Center of the Storm*, January 2017, p. 2. Available at https://www.mandiant.com/resources/reports/apt28-center-storm (accessed August 2023).
- Foreign Affairs Committee, House of Commons, 'Oral Evidence: Use of Strategic Lawsuits against Public Participation, HC 1196', 15 March, 2022, Q 21. Available at https://committees.parliament.uk/oralevidence/9907/pdf/ (accessed August 2023).

- Galeotti, M., 'Active Measures: Russia's Covert Geopolitical Operations', George C. Marshall European Center For Security Studies, June 2019. Available at https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0 (accessed August 2023).
- Global Times, 'US NED "Mastermind" behind Global Separatist Riots, Color Revolutions, Political Crises: Chinese FM Report', 8 May, 2022. Available at https://www.globaltimes.cn/page/202205/1265027.shtml (accessed August 2023).
- Charon, P., Jeangène Vilmer, J.B., *Chinese Influence Operations*, Report by the Institute for Strategic Research (IRSEM), Paris, Ministry for the Armed Forces, October 2021. Available at https://www.irsem.fr/report.html (accessed August 2023).
- Grimes, D. R., 'Russian Misinformation Seeks to Confound, Not Convince', Scientific American, 28 March, 2022. Available at https://www.scientificamerican.com/article/russian-misinformation-seeks-to-confound-not-convince/ (accessed August 2023).
- Harper, J., 'Attorneys as State Actors: A State Action Model and Argument for Holding SLAPP-Plaintiffs' Attorneys Liable under 42 U.S.C. 1983', *UC Law Constitutional Quarterly*, Vol. 21, No. 2, 1 January, 1994, p. 405.
- Hartcher, P., 'Sam Dastyari: Riding the Red Dragon Express Not a Good Look', The Sydney Morning Herald, 3 September, 2016. Available at https://www.smh.com.au/opinion/sam-dastyari-riding-the-red-dragon-express-not-a-good-look-20160902-gr7tcy.html (accessed August 2023).
- Henderson, S., Miller, S., Perez, D., Siedlarz, M., Wilson, B., Read, B., 'Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally', Mandiant, 10 July, 2018. Available at https://www.mandiant.com/resources/blog/chinese-espionage-group-targets-cambodia-ahead-of-elections (accessed August 2023).
- Huntley, S., 'How We're Tackling Evolving Online Threats', Google Threat Analysis Group (TAG), 16 October, 2020. Available at https://blog.google/threat-analysis-group/how-were-tackling-evolving-online-threats/ (accessed August 2023).
- Hurst, D., Kuo, L., Graham-McLay, C., 'Zhenhua Data Leak: Personal Details of Millions around World Gathered by China Tech Company', The Guardian, 14 September, 2020. Available at https://www.theguardian.com/world/2020/sep/14/zhenhua-data-full-list-leak-database-personal-details-millions-china-tech-company (accessed August 2023).
- Intelligence and Security Committee of UK Parliament, 'Russia', 21 July, 2020, pp. 12-14. Available at https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf (accessed August 2023).

- Janeliūnas, T., Boruta, R., 'Lithuania's Confrontation with China Over Taiwan: Lessons from a Small Country', Global Taiwan Institute, 27 July, 2022. Available at https://globaltaiwan.org/2022/07/lithuanias-confrontation-with-china-over-taiwan-lessons-from-a-small-country/ (accessed August 2023).
- Jeangène Vilmer, J.B., Escorcia, A., Guillaume, M., Herrera, J., *Information Manipulation: A Challenge for Our Democracies*, Report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, August 2018. Available at https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf (accessed August 2023).
- Jeangène Vilmer, J.B., *The 'Macron Leaks' Operation: A Post-Mortem*, Atlantic Council Policy, June 2019. Available at https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf (accessed August 2023).
- Jensen, P.S., Justesen, M.K., 'Poverty and Vote Buying: Survey-Based Evidence from Africa', *Electoral Studies,* Vol. 33, March 2014, pp. 220–232.
- Joseph, O., Vashchanka, V., *Vote Buying: International IDEA Electoral Processes Primer 2*, International Institute for Democracy and Electoral Assistance (International IDEA), 2022. Available at https://www.idea.int/publications/catalogue/vote-buying (accessed August 2023).
- Jung, H.M., 'Information Manipulation Through the Media', *Journal of Media Economics*, Vol. 22, No. 4, 30 November, 2009, pp. 188–210.
- Jung, C., 'China's Interference in Canada's Election', The Diplomat, 22 November, 2022. Available at https://thediplomat.com/2022/11/chinas-interference-in-canadas-elections/ (accessed August 2023).
- Karásková, I., *Analysing China Radio International's Tactics: A Case Study of Narratives Disseminated in the Czech Republic*, The Central European Digital Media Observatory (CEDMO), June 2023, p. 4. Available at https://cedmohub.eu/wp-content/uploads/2023/06/EN_Espresso.pdf (accessed August 2023).
- Karásková, I., et al., *Backing Russia on Ukraine: China's Messaging in Central and Eastern Europe*, Association for International Affairs (AMO), Prague, Czech Republic, May 2022.
- Karásková, I., et al., *China's Sticks and Carrots in Central Europe: The Logic and Power of Chinese Influence*, Association for International Affairs (AMO), 2020.
- Keating, D., 'EFDD 'Smear Campaign' Used Russian Help', POLITICO, 29 January, 2015. Available at https://www.politico.eu/article/efdd-smear-campaign-used-russian-help/ (accessed August 2023).
- Homeland Security, 'Key Findings and Recommendations from the Joint Report of the Department of Justice and the Department of Homeland Security on Foreign Interference Targeting Election Infrastructure or Political Organization, Campaign, or Candidate

Infrastructure Related to the 2020 US Federal Elections', March 2021. Available at https://www.dhs.gov/publication/key-findings-and-recommendations-foreign-interference-related-2020-us-federal-elections (accessed August 2023).

- Korsunskaya, D., 'Putin Says Russia Must Prevent "Color Revolution"', Reuters, 20 November, 2014. Available at https://www.reuters.com/article/us-russia-putin-security-idUSKCN0J41J620141120 (accessed August 2023).
- Kurlantzick, J., 'China's War for Hearts and Minds', Washington Monthly, 3 March, 2023. Available at http://washingtonmonthly.com/2023/03/03/chinas-war-for-hearts-and-minds/ (accessed August 2023).
- Lageman, T., 'Russian Hackers and the Dutch Election', Deutsche Welle, 3 October, 2017. Available at https://www.dw.com/en/russian-hackers-use-dutch-polls-as-practice/a-37850898 (accessed August 2023).
- Lamb, K., 'Indonesia Election Mired in Claims of Foreign Hacking and 'ghost' Voters', The Guardian, 19 March, 2019. Available at https://www.theguardian.com/world/2019/mar/19/indonesia-election-mired-in-claims-of-foreign-hacking-and-ghost-voters (accessed August 2023).
- Lamond, J., Dessel, T., 'Democratic Resilience A Comparative Review of Russian Interference in Democratic Elections and Lessons Learned for Securing Future Elections', Center for American Progress, September 2019. Available at https://www.americanprogress.org/article/democratic-resilience/ (accessed August 2023).
- Lavalette, T., 'Australia Investigates China Plot to Plant Spy in Parliament', AP News, 25 November, 2019. Available at https://apnews.com/article/f60823ab8cc74803bb687d25c54824bf (accessed August 2023).
- Leonard, M., Bachulska, A., 'China and Ukraine: The Chinese Debate about Russia's War', Policy Brief, European Council on Foreign Relations, 11 July, 2023. Available athttps://ecfr.eu/publication/china-and-ukraine-the-chinese-debate-about-russias-war-and-its-meaning-for-the-world/ (accessed August 2023).
- Levin, D. H., *Meddling in the Ballot Box: The Causes and Effects of Partisan Electoral Interventions*, 1st ed., Oxford University Press, 2020.
- Levin, D. H., 'Will You Still Love Me Tomorrow? Partisan Electoral Interventions, Foreign Policy Compliance, and Voting in the UN', *International Interactions*, Vol. 47, No. 3, 4 May, 2021, pp. 449-476.
- Lim, Y., 'Election Cyber Threats in the Asia-Pacific Region', Mandiant, 22 November, 2020. Available at https://www.mandiant.com/resources/blog/election-cyber-threats-in-the-asia-pacific-region (accessed August 2023).
- Lin, C., '退將羅文山涉收政治獻金 金主是中共全國政協委員', 中央社 CNA, 3 December, 2019. Available at https://www.cna.com.tw/news/firstnews/201912030181.aspx (accessed August 2023).

- LOI N° 2018-1202 Du 22 Décembre 2018 Relative à La Lutte Contre La Manipulation de l'information (1). Available at https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037847559 (accessed August 2023).
- Mackin, B., 'Update: Vancouver City Hall Refers WeChat Vote-Buying Scheme to Police', TheBreaker, 12 October, 2018. Available at https://thebreaker.news/news/wechat-wenzhou/ (accessed August 2023).
- Mandiant, 'UNC1151 Assessed to Have Links to Belarusian Government', 16 November, 2021. Available at https://www.mandiant.com/resources/blog/unc1151-linked-to-belarus-government (accessed August 2023).
- Mares, I., Muntean, A., Petrova,T., 'Pressure, Favours, and Vote-Buying: Experimental Evidence from Romania and Bulgaria', *Europe-Asia Studies*, Vol. 69, No. 6, 3 July, 2017, pp. 940–960.
- Marks,J., 'Is Russia or China the Biggest Cyber Threat? Experts Are Split', Washington Post, 20 January, 2022. Available at https://www.washingtonpost.com/politics/2022/01/20/is-russia-or-china-biggest-cyber-threat-experts-are-split/ (accessed August 2023).
- Martin, D.A., Shapiro, J.N., Ilhardt, J.G., 'Online Political Influence Efforts Dataset, Version 4.0', 24 March, 2023. Available at https://esoc.princeton.edu/publications/trends-online-influence-efforts (accessed August 2023).
- Massola, J., 'Chinese Donor the Yuhu Group Steps in to Help Sam Dastyari', The Sydney Morning Herald, 27 March, 2015. Available at https://www.smh.com.au/politics/federal/chinese-donor-the-yuhu-group-steps-in-to-help-sam-dastyari-20150327-1m9be2.html (accessed August 2023).
- McKenzie, N., Baker, R., Uhlmann, C., 'Liberal Andrew Robb Took $880k China Job as Soon as He Left Parliament', The Sydney Morning Herald, 6 June, 2017. Available at https://www.smh.com.au/national/liberal-andrew-robb-took-880k-china-job-as-soon-as-he-left-parliament-20170602-gwje3e.html (accessed August 2023).
- McKenzie, N., Massola, J., Baker, R., '"It Isn't Our Place": New Tape of pro-Beijing Comments Puts More Heat on Dastyari', The Sydney Morning Herald, 29 November, 2017. Available at https://www.smh.com.au/politics/federal/it-isnt-our-place-new-tape-of-probeijing-comments-puts-more-heat-on-dastyari-20171128-gzuiup.html (accessed August 2023).
- McNamara, L., 'Framing the Problem: Cyber Threats and Elections', Mandiant, 30 May, 2019. Available at https://www.mandiant.com/resources/blog/framing-problem-cyber-threats-and-elections (accessed August 2023).
- Merchant, N., Lee, M., 'US Sees China Propaganda Efforts Becoming More Like Russia's', AP News, 7 March, 2023. Available at https://apnews.com/article/china-russia-intelligence-foreign-influence-propaganda-0476f41aa932cd4850627a7b8984baa2 (accessed August 2023).

- Meta, 'Removing Coordinated Inauthentic Behavior from China and Russia', 27 September, 2022. Available at https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/ (accessed August 2023).
- Microsoft, Microsoft Digital Defense Report 2022, 2022. Available at https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022 (accessed August 2023).
- Mohan, V., Wall, A., 'Foreign Electoral Interference: Past, Present, and Future', Georgetown *Journal of International Affairs*, Vol. 20, 2019, p. 110.
- Mosk, M., Turner, T., Faulders, K., 'Russian Influence Operation Attempted to Suppress Black Vote: Indictment', 18 February, 2018. Available at https://abcnews.go.com/Politics/russian-influence-operation-attempted-suppress-black-vote-indictment/story?id=53185084 (accessed August 2023).
- National Assembly of the French Republic, 'Rapport fait au nom de la commission d'enquête, relative aux ingérences politiques, économiques et financières de puissances étrangères – États, organisations, entreprises, groupes d'intérêts, personnes privées – visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques français', 1 June, 2023. Available at https://www.assemblee-nationale.fr/dyn/16/rapports/ceingeren/l16b1311-t1_rapport-enquete (accessed August 2023).
- National Intelligence Council, 'Foreign Threats to the 2020 US Federal Elections, National Intelligence Council', 10 March, 2021. Available at https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf (accessed August 2023).
- Neidhardt, A.H., *Disinformation on Refugees from Ukraine: Boosting Europe's Resilience after Russia's Invasion*, Foundation for European Progressive Studies (FEPS), 2022. Available at https://feps-europe.eu/wp-content/uploads/2022/12/PS-Disinformation.pdf (accessed August 2023).
- Newman, L.H., 'Security News This Week: A Destabilizing Hack-and-Leak Operation Hits Moldova', Wired, 19 October, 2022. Available at https://www.wired.com/story/moldova-leaks-google-privacy-settlement-world-cup-apps/ (accessed August 2023).
- Nimmo, B., Torrey, M., 'Taking down Coordinated Inauthentic Behavior from Russia and China', Meta, September 2022. Available at https://www.politico.eu/wp-content/uploads/2022/09/27/NEAR-FINAL-DRAFT-CIB-Report-ChinaRussia-Sept-2022.pdf (accessed August 2023).
- Noack, R., 'Everything We Know So Far about Russian Election Meddling in Europe', Washington Post, 10 January, 2018. Available at https://www.washingtonpost.com/news/worldviews/wp/2018/01/10/everything-we-know-so-far-about-russian-election-meddling-in-europe/ (accessed August 2023).

- Nuttall, J., 'Death Threats against Chinese Canadian Who Spoke out on Uyghur Genocide Claims Must Be Investigated, Say B.C. Community Leaders', Toronto Star, 14 April, 2021. Available at https://www.thestar.com/news/canada/death-threats-against-chinese-canadian-who-spoke-out-on-uyghur-genocide-claims-must-be-investigated/article_38720cec-b76b-51cf-a602-48407d6268c9.html (accessed August 2023).
- O'Connor, S., Hanson, F., Currey, E., and Beattie, T., *Cyber-Enabled Foreign Interference in Elections and Referendums*, The Australian Strategic Policy Institute, October 2020, pp.31-45. Available at https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums (accessed August 2023).
- O'Malley, N., Joske. A., 'Mysterious Bennelong Letter Urges Chinese Australians to "take down" the Turnbull Government', The Sydney Morning Herald, 13 December, 2017. Available at https://www.smh.com.au/politics/federal/mysterious-bennelong-letter-urges-chinese-australians-to-take-down-the-turnbull-government-20171213-h03pc4.html (accessed August 2023).
- O'Sullivan, D., 'Russian Hackers Targeting European Governments before Elections, Security Firm Warns', CNN, 22 March, 2019. Available at https://www.cnn.com/2019/03/22/europe/russia-hackers-european-elections-intl/index.html (accessed August 2023).
- Paganini, P., 'The Dutch Intelligence Service AIVD "Hacked" Russian Cozy Bear Systems for Years', Security Affairs, 26 January, 2018. Available at https://securityaffairs.com/68241/intelligence/aivd-hacked-cozy-bear.html (accessed August 2023).
- Page, C., 'EU Warns Russia over "Ghostwriter" Hacking Ahead of German Elections', TechCrunch, 24 September, 2021. Available at https://techcrunch.com/2021/09/24/european-council-russia-ghostwriter/ (accessed August 2023).
- Pennings, F., 'Cyber Resilience Act: A Step towards Safe and Secure Digital Products in Europe', Microsoft, 16 February, 2023. Available at https://blogs.microsoft.com/eupolicy/2023/02/16/cyber-resilience-act-cybersecurity-skills/ (accessed August 2023).
- Polyakova, A., Meserole, C., *Exporting Digital Authoritarianism: The Russian and Chinese Models*, Brookings Institution, 2019, p. 2. Available at https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf (accessed August 2023).
- Public Broadcasting of Latvia, 'Draugiem.Lv Social Network Hacked with pro-Russia Message', 6 October, 2018. Available at https://eng.lsm.lv/article/society/crime/draugiemlv-social-network-hacked-with-pro-russia-message.a294979/ (accessed August 2023).
- 'Putin's People: Settlement Reached in Roman Abramovich v HarperCollins and Catherine Belton', Corporate.Harpercollins.Co.Uk, 22 December, 2021. Available at

https://corporate.harpercollins.co.uk/press-releases/putins-people-settlement-reached-in-roman-abramovich-v-harpercollins-and-catherine-belton/ (accessed August 2023).

- PwC, *Cyber Threats 2022: A Year in Retrospect*, 2023. Available at https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html (accessed August 2023).
- Qian, L., '中國策動台商資助介選 中南部企業涉入 調局立案蒐證', Liberty Times Net, 24 April, 2023. Available at https://news.ltn.com.tw/news/politics/paper/1579196 (accessed August 2023).
- Ramos, J. M., and Raab, N., 'Russia Abroad, Russia at Home: The Paradox of Russia's Support for the Far Right', *Russian Politics*, Vol. 7, No. 1, 8 March, 2022, pp. 80-81.
- Rankin, J., 'EU Says China behind 'huge Wave' of Covid-19 Disinformation', The Guardian, 10 June, 2020. Available at https://www.theguardian.com/world/2020/jun/10/eu-says-china-behind-huge-wave-covid-19-disinformation-campaign (accessed August 2023).
- Ravindranath, M., 'Russia Wanted to Be Caught, Says Company Waging War on the DNC Hackers - Defense One', Defense One, 27 July, 2016. Available at https://www.defenseone.com/technology/2016/07/Russia-wanted-to-be-caught/130312/ (accessed August 2023).
- 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 ('Regulation 1141/2014'). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R1141 (accessed August 2023).
- Reimann, N., 'Foreign Electoral Interference Normative Implications in Light of International Law, Human Rights, and Democratic Theory', Dissertation, University of Zurich, 2023, p. 29. Available at https://www.zora.uzh.ch/id/eprint/233343/ (accessed August 2023).
- Reporters Without Borders, 'Baltic Countries: Misusing EU Sanctions to Ban Russian TV Channels Is Not a Legitimate Tool for Promoting Reliable Information', 10 July, 2020. Available at https://rsf.org/en/baltic-countries-misusing-eu-sanctions-ban-russian-tv-channels-not-legitimate-tool-promoting (accessed August 2023).
- Reuters, 'Czech Election Websites Hacked, Vote Unaffected - Statistics Office', 22 October, 2017. Available at https://www.reuters.com/article/czech-election-cyber-idUSL8N1MX0OB (accessed August 2023).
- Reuters, 'Exclusive: Australia Concluded China Was behind Hack on Parliament, Political Parties – Sources', 15 September, 2019. Available at https://www.reuters.com/article/us-australia-china-cyber-exclusive-idUSKBN1W00VF (accessed August 2023).
- Riley, M., Robertson, J., 'Russian Hacks on US Voting System Wider Than Previously Known', Bloomberg, 13 June, 2017. Available at https://www.bloomberg.com/politics/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections (accessed August 2023).

- Rosenberg, M., Singer, D.E., Perlroth, N., '"Chaos Is the Point": Russian Hackers and Trolls Grow Stealthier in 2020', 10 January, 2020. Available at https://www.nytimes.com/2020/01/10/us/politics/russia-hacking-disinformation-election.html (accessed August 2023)
- Sakkal, P., McKenzie, N., 'Death of Melbourne-Based Chinese Spy Target "not Suspicious" Says Coroner', The Age, 21 September, 2020. Available at https://www.theage.com.au/national/victoria/death-of-melbourne-based-fraudster-not-suspicious-says-coroner-20200921-p55xmd.html (accessed August 2023).
- Salvi, E., Suc, M., Turchi, M., 'Un rapport parlementaire révèle dix ans de connivence entre la Russie et le RN', Mediapart, 1 June, 2023. Available at https://www.mediapart.fr/journal/politique/010623/un-rapport-parlementaire-revele-dix-ans-de-connivence-entre-la-russie-et-le-rn (accessed August 2023).
- Santora, M., Barnes, J.E., 'In the Balkans, Russia and the West Fight a Disinformation-Age Battle', The New York Times, 16 September, 2018. Available at https://www.nytimes.com/2018/09/16/world/europe/macedonia-referendum-russia-nato.html (accessed August 2023).
- Secretariat-General for National Defence and Security, *RNN: A Complex and Persistent Digital Information Manipulation Campaign*, 19 July, 2023, p.17. Available at https://www.sgdsn.gouv.fr/files/files/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN1.pdf (accessed August 2023).
- Serrano-Puche, J., 'Digital Disinformation and Emotions: Exploring the Social Risks of Affective Polarization', *International Review of Sociology*, Vol. 31, No. 2, 4 May, 2021, pp. 231–245.
- Sheikin, A., ‚Информационная война', council.gov.ru, 21 June, 2022. Available at http://council.gov.ru/services/discussions/blogs/136503/ (accessed August 2023).
- Sherman, J., 'Changing the Kremlin's Election Interference Calculus', *The Washington Quarterly*, Vol. 45, No. 1, 2 January, 2022, p. 120.
- Schechner, S., 'France Says Evidence Suggests Russians Posing as Islamists Hacked Broadcaster', The Wall Street Journal, 10 June, 2015. Available at https://www.wsj.com/articles/france-says-evidence-suggests-russians-posing-as-islamists-hacked-broadcaster-1433955381 (accessed August 2023).
- Schmitt, G., Mazza, M., *Blinding the Enemy: CCP Interference in Taiwan's Democracy*, Global Taiwan Institute, October 2019. Available at https://globaltaiwan.org/wp-content/uploads/2022/08/GTI-CCP-Interference-Taiwan-Democracy-Oct-2019-final.pdf (accessed August 2023).
- Smith, B., 'Defending Ukraine: Early Lessons from the Cyber War', Microsoft, June 22, 2022. Available at https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/ (accessed August 2023).

- Sonne, P., 'A Russian Bank Gave Marine Le Pen's Party a Loan. Then Weird Things Began Happening', Washington Post, 29 December, 2018. Available at https://www.washingtonpost.com/world/national-security/a-russian-bank-gave-marine-le-pens-party-a-loan-then-weird-things-began-happening/2018/12/27/960c7906-d320-11e8-a275-81c671a50422_story.html (accessed August 2023).
- Soula, E., 'The Many Faces of Foreign Interference in European Elections', German Marshall Fund of the United States. Available at https://www.gmfus.org/news/many-faces-foreign-interference-european-elections (accessed August 2023).
- Sp-agency.ru, 'ДИГИТАТОР', Available at https://sp-agency.ru/tools/9/ (accessed August 2023).
- Starr, P., 'The Flooded Zone: How We Became More Vulnerable to Disinformation in the Digital Era', in Bennett, W.L., Livingston, S. (eds.), *The Disinformation Age*, 1st ed., Cambridge University Press, Cambridge, 2020.
- State Security Department of the Republic of Lithuania and Defence Intelligence and Security Service under the Ministry of National Defence, 'National Threat Assessment 2023'. Available at https://kam.lt/wp-content/uploads/2023/03/Assessment-of-Threats-to-National-Security-2022-published-2023.pdf (accessed August 2023).
- Stelzenmüller, C., 'The Impact of Russian Interference on Germany's 2017 Elections', Brookings Institution, 28 June, 2017. Available at https://www.brookings.edu/articles/the-impact-of-russian-interference-on-germanys-2017-elections/ (accessed August 2023).
- Tennis, M., 'Russia Ramps up Global Elections Interference: Lessons for the United States', Center for Strategic and International Studies (CSIS), 20 July, 2020. Available at https://www.csis.org/blogs/strategic-technologies-blog/russia-ramps-global-elections-interference-lessons-united-states (accessed August 2023).
- The European Union Agency for Cybersecurity (ENISA), *Election Cybersecurity: Challenges and Opportunities*, February 2019. Available at https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/election-cybersecurity-challenges-and-opportunities (accessed August 2023).
- Global Times, 'Lithuanian Politicians, Nathan Law Are West's Tools to Do 'Dirty Work"', 24 November, 2021. Available at https://www.globaltimes.cn/page/202111/1239862.shtml (accessed August 2023).
- The Atlantic Council, 'Foreign Interference in Ukraine's Democracy', 15 May, 2019. Available at https://www.atlanticcouncil.org/in-depth-research-reports/report/foreign-interference-in-ukraine-s-election/ (accessed Auguste 2023).
- The European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2022*, October 2022. Available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (accessed August 2023).

- The Globe and Mail, 'CSIS Documents Reveal Chinese Strategy to Influence Canada's 2021 Election', 17 February, 2023. Available at https://www.theglobeandmail.com/politics/article-china-influence-2021-federal-election-csis-documents/ (accessed August 2023).
- The Observers - France 24, 'An Iranian Tries to Sell His Vote on EBay', The Observers - France 24, 14 June, 2013. Available at https://observers.france24.com/en/20130614-iranian-tries-sell-vote-ebay (accessed August 2023).
- Tomz, M., Weeks, J., 'Public Opinion and Foreign Electoral Intervention', *American Political Science Review*, Vol. 114, No. 3, August 2020.
- United States District Court, District of Columbia, 17 October, 2017, *Deripaska v. Associated Press,* 282 F. Supp. 3d 133. Available at https://casetext.com/case/deripaska-v-associated-press (accessed August 2023).
- United States Senate, 'Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 US Election', Volume 1: Russian Efforts Against Election Infrastructure with Additional Views', 10 November, 2020. Available at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf (accessed August 2023).
- US Department of Justice, Office of Public Affairs, 'Former Head of Organization Backed by Chinese Energy Conglomerate Sentenced to Three Years in Prison for International Bribery and Money Laundering Offenses' [Press Release], 25 March, 2019. Available at https://www.justice.gov/opa/pr/former-head-organization-backed-chinese-energy-conglomerate-sentenced-three-years-prison (accessed August 2023).
- US Department of Justice , 'Report On The Investigation Into Russian Interference In The 2016 Presidential Election', Volume I of II, March 2019, p. 14. Available at https://www.justice.gov/archives/sco/file/1373816/download (accessed August 2023).
- Usta, B., 'Erdogan Tells Turks in Germany to Vote against Merkel', Reuters, 18 August, 2017. Available at https://www.reuters.com/article/us-germany-Türkiye-idUSKCN1AY17Z (accessed August 2023).
- Valášek, L., Truchlá, H., '"Four Million for Vystrčil": Chinese Attempt at Disparaging President of Czech Senate', Aktuálně, 11 November, 2020. Available at https://zpravy.aktualne.cz/domaci/four-million-dollars-for-vystrcil-chinese-attempt-at-dispara/r~1808fbea245111eb95caac1f6b220ee8/ (accessed August 2023).
- Van Der Staak, S., Wolf, P., *Cybersecurity in Elections: Models of Interagency Collaboration*, International Institute for Democracy and Electoral Assistance, 2019. Available at https://www.idea.int/publications/catalogue/cybersecurity-in-elections (accessed August 2023).
- Vosoughi, S., Roy, D., Aral, S., 'The Spread of True and False News Online', *Science*, Vol. 359, No. 6380, 9 March, 2018, pp. 1146–1151. Available at https://www.science.org/doi/10.1126/science.aap9559 (accessed August 2023).

- Wang, Y., 'China's Overseas Critics under Pressure from Smear Campaigns, Cyber Attacks', Committee to Protect Journalists, 11 March, 2016. Available at https://cpj.org/2016/03/chinas-overseas-critics-under-pressure-from-smear/ (accessed August 2023).
- Watts, C., 'Who Cares about a Midterm Election? Comparing Russia, Iran, and China's Electoral Interference from Past to Present', Alliance for Securing Democracy - German Marshall Fund, 19 May, 2022. Available at https://securingdemocracy.gmfus.org/who-cares-about-a-midterm-election-comparing-russia-iran-and-chinas-electoral-interference-from-past-to-present/ (accessed August 2023).
- Weber, R., *Unified message, rhizomatic delivery. A preliminary analysis of PRC/CCP influence and the united front in Switzerland,* Sinopsis – China in Context and Perspective, 2020.
- Wilson, K.L., 'Strategic Responses to Chinese Election Interference in Taiwan's Presidential Elections', *Asian Perspective*, Vol. 46, No. 2, March 2022, pp. 255–277.
- Winder, D., 'Linux Security: Chinese State Hackers May Have Compromised "Holy Grail" Targets Since 2012', Forbes, 7 April, 2020. Available at https://www.forbes.com/sites/daveywinder/2020/04/07/linux-security-chinese-state-hackers-have-compromised-holy-grail-targets-since-2012/ (accessed August 2023).
- Wong, E., 'Russia Secretly Gave $300 Million to Political Parties and Officials Worldwide, US Says', The New York Times, 13 September, 2022. Available at https://www.nytimes.com/2022/09/13/us/politics/russia-election-interference.html (accessed August 2023).
- Yates, W., 'Jessikka Aro: How pro-Russian Trolls Tried to Destroy Me - BBC News', BBC News, 6 October, 2017. Available at https://www.bbc.com/news/blogs-trending-41499789 (accessed August 2023).
- Youtube, 'Ran Shahor Cyber Week 2022', 2022. Available at https://www.youtube.com/watch?v=CC9meMEesAk (accessed August 2023).
- Zambrano, D. A., 'Foreign Dictators in US Court', The University of Chicago Law Review, Vol. 89, No. 1, 1 January, 2022, pp. 157–252. Available at https://www.jstor.org/stable/pdf/27093694.pdf?casa_token=4_D13E0hpOQAAAAA:MaHwnW3qFpEOfni5IEiETwK168ag6XeG0mGqOQ_Vu2Rpf8obQKcF6vRPZYhUp44_MCHDnT-F-TBeYrtN9U3GUQva9Nq9mXvFOwtgsSRrGv0P0OMvdxMF (accessed August 2023).
- Zambrano, D. A., 'Testimony Before the US-China Economic and Security Review Commission', 4 May, 2023. Available at https://www.uscc.gov/sites/default/files/2023-05/Diego_Zambrano_Testimony.pdf (accessed August 2023).
- Zhao, L. 赵立坚 [@zlj517], 'CDC Was Caught on the Spot. When Did Patient Zero Begin in US? How Many People Are Infected? What Are the Names of the Hospitals? It Might Be US Army Who Brought the Epidemic to Wuhan. Be Transparent! Make Public Your Data! US Owe Us an Explanation!' [Tweet], Twitter, 12 March, 2020. Available at https://Twitter.com/zlj517/status/1238111898828066823?lang=en (accessed August 2023).

- Zhao, L. 赵立坚 [@zlj517], 'This Article Is Very Much Important to Each and Every One of Us. Please Read and Retweet It. COVID-19: Further Evidence That the Virus Originated in the US.' [Tweet], Twitter, 13 March, 2020. Available at https://Twitter.com/zlj517/status/1238269193427906560 (accessed August 2023).

Malign foreign state and non-state actors employ intricate strategies to manipulate elections, including in Europe. This study sets out the toolbox of malign actors affecting the EU. It delves into financial incentives, information manipulation, and cyber interventions, all while spotlighting Russia and China's roles.