IN-DEPTH ANALYSIS

Requested by the INGE committee

European Parliament

The misuse of social media platforms and other communication channels by authoritarian regimes: Lessons learned

Authors:

Lukas ANDRIUKAITIS, Jakub KALENSKY, Simin KARGAR, Elene PANCHULIDZE, Joanna SMĘTEK, Anastas VANGELI

European Parliament coordinator:

Policy Department for External Relations

Directorate General for External Policies of the Union

PE 653.658 - December 2021

EN

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES
POLICY DEPARTMENT

European Parliament

In-depth analysis

The misuse of social media platforms and other communication channels by authoritarian regimes: Lessons learned

ABSTRACT

Disinformation has continued to spread in recent years, receiving a significant boost during the COVID-19 pandemic and constituting one of the most pressing threats for democratic countries. Authoritarian regimes have played their part in the proliferation of manipulated content, particularly disinformation. This paper analyses recent instances of the misuse of social media platforms and other communication channels perpetrated by authoritarian regimes in Iran, China, and Russia to influence the public opinion and democratic processes in Yemen and Syria, Taiwan, and Georgia, respectively, focusing on disinformation in particular. The authors draw lessons for the EU in relation to the actors involved, highlighting the impact of disinformation, the disparity of resources between perpetrators and responders, and the importance of independent media and a whole-of-society approach. By juxtaposing local experiences with analysis of EU instruments, the authors arrive at a set of recommendations, which highlight the need to: focus on various disinformation perpetrators beyond Russia; support independent media and civil society initiatives; collect comparable data within the EU; develop mechanisms targeting perpetrators and increasing the cost of engaging in disinformation; develop proactive and pre-emptive campaigns against disinformation; and increase coordination and cooperation within the EU around the issue of disinformation.

EP/EXPO/INGE/FWC/2019-01/LOT4/1/C/09
December 2021 - PE 653.658

EN

Policy Department, Directorate-General for External Policies

AUTHORS

- Lukas ANDRIUKAITIS, Associate Director at Atlantic Council's Digital Forensic Research Lab (Chapters 1-2)
- Jakub KALENSKY, Senior Fellow, Digital Forensic Research Lab, Atlantic Council (Chapters 4-6, Annex 1)
- Simin KARGAR, Non-resident fellow, Digital Forensic Research Lab, Atlantic Council; PhD researcher at Johns Hopkins University (Chapter 3, Iran case study)
- Elene PANCHULIDZE, Independent Consultant (Chapter 3, Russia case study)
- Joanna SMĘTEK, International Research Team, Ecorys Poland (Chapters 1-2)
- Anastas VANGELI, Assistant Professor, School of Economics and Business, University of Ljubljana, Slovenia (Chapter 3, China case study)

PEER REVIEWER

Dr Ofer FRIDMAN, Senior Lecturer in War Studies, King's College London, United Kingdom

PROJECT COORDINATOR (CONTRACTOR)

- Joanna SMĘTEK, ECORYS Poland; Katarzyna LUBIANIEC, Ecorys Poland

This paper was requested by the European Parliament's Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation

CONTACTS IN THE EUROPEAN PARLIAMENT

Coordination: Andrea MAIER, Policy Department for External Policies

Editorial assistant: Grégory DEFOSSEZ

Feedback is welcome. Please write to andrea.maier@europarl.europa.eu

To obtain copies, please send a request to poldep-expo@europarl.europa.eu

English-language manuscript completed on 1 December 2021

COPYRIGHT

This paper will be published on the European Parliament's online database, 'Think Tank'

Table of contents

Executive summary

Purpose and scope of the paper

The paper examines ways in which authoritarian regimes in Iran, China, and Russia have used social media and other communication channels to influence the public opinion and interfere in democratic processes in Yemen and Syria, Taiwan and Georgia. The goal of this analysis is to increase understanding of such mechanisms through specific examples; to draw lessons both from local and European Union (EU) perspectives; and to recommend ways in which the EU can improve its instruments and actions to respond to similar efforts of outside, authoritarian regimes spreading messages within the EU. Accordingly, the case studies describe examples of recent misuse, specifying the communication channels and methods applied, as well as the measures adopted by the targeted authorities or local non-state actors to address interferences and mitigate their impact. The experiences studied have been used to analyse and assess the EU instruments relevant for misuse of social media and other communication channels, particularly those focused on disinformation. The paper considers how well these instruments would respond to the methods employed by external authoritarian regimes and whether they are adapted to implement best practices, as revealed in the case studies. The paper then considers what the EU can learn from local experiences, and draws specific EU-level lessons which are coupled with recommendations for EU actors in various dimensions of EU actions.

The case of Iran/Yemen and Syria

Since the formation of the Islamic Republic in 1979, Iran's foreign policy of "exporting the revolution" has guided the country's transnational media and outreach operations. These measures continue to evolve with advancements in media and communication technologies, making Iran one of the most prolific threat actors in the Middle East. Iran's weaponisation of social media is part of a broader scheme for influence in states with strategic value to Iran's foreign policy. Its social media operations occur in tandem with media broadcasting, on-the-ground promotional activities, recruiting Shi'a minorities on an ideological basis, and supporting business operations for post-war reconstruction in countries like Syria. In this puzzle, Iran's information influence operations through social media and other vehicles are an indicator of how Iran pursues its national interests and foreign policy priorities. These operations often propagate pro-Iran narratives through front media and their social media platforms to maximise reach. Since 2018, Facebook and Twitter have suspended networks of Iran-affiliated accounts. However, countering the narratives that Iran systematically promotes in Yemen and Syria requires comprehensive multi-stakeholder efforts that tackle different aspects of these operations. Government responses in both countries have been lacking due to low capacity and geopolitical situations. Civil society has put forward a few initiatives, but lacks the necessary resources.

The case of China and Taiwan

The People's Republic of China's (PRC) reach into Taiwan's media space takes place in various forms. In the wake of the 2019 protests in Hong Kong, a large network of inauthentic accounts on social media networks based in Mainland China was identified. Some of them have been taken down by Facebook, Twitter, and YouTube on the grounds of being connected with the PRC. This network has nevertheless endured, remaining active around the 2020 elections, and likely during the COVID-19 pandemic. It has not had significant success in achieving their goals, however.

The rise of the content creator economy has provided another opportunity for the PRC to bankroll questionable content through donations to content creators on YouTube and other platforms. Disinformation spread through these various channels often intersects with commercial interests, and extends into areas beyond politics (most commonly, personal health).The importance of PRC impact

notwithstanding, in the run up to the 2020 general election it became evident that internal divisions between political parties are another key driver of disinformation on social media.

Taiwan has taken measures, including a number of legislative actions, to address the threat arising from external influence since its democratic opening in the late 1980s. The most significant recent piece of legislation under the Democratic Progressive Party government was the adoption of the Anti-Infiltration Act (AIA) on 31 December 2019, which primarily focuses on linkages of political actors to foreign entities. A game changer in Taiwan's struggle against disinformation, however, has been Digital Minister Audrey Tang, who devised a proactive and inclusive (whole-of-society) approach based on pre-emption, and early and rapid response, which rests on collaboration with social media companies to tackle viral disinformation content on their platforms; support of fact-checking services and databases; and transparent and inclusive governance. Civil society and 'civic tech' mobilisation has also played a significant role.

In Taiwan, one best practice is that response to the spread of questionable content does not revolve around censorship or sanctioning, but rather around a proactive, engaging strategy that involves different actors (e.g. social media platforms, government, civic tech activists, and fact-checkers), and which combines technology-oriented solutions with human creative power.

The case of Russia/Georgia

Russia's efforts to interfere in Georgia's democratic processes and influence public opinion have long been prevalent, but intensified following the 2008 military aggression and illegal occupation of Georgian territories. Yet military aggression is only one dimension of Russia's attempts to influence the domestic and foreign politics of Georgia. Russia's disinformation and dissemination of anti-Western narratives in the public information space are at odds with Georgia's national interests, including its Euro-Atlantic integration process. Over the years, Russian information operations have evolved and adapted, with activities becoming more covert and harder to detect. Social media platforms, with fractional monitoring and regulatory frameworks, have become increasingly popular channels for the dissemination and manipulation of content that has allowed Russia to further expand its disinformation outreach. Limited institutional capacity and feeble strategic communications weaken Georgia's efforts to protect the public information space from Russian interference. Political turbulence, internal disinformation, and the absence of a whole-of-society approach against Russian disinformation all make Georgia particularly vulnerable to ongoing foreign disruptive meddling. A number of actions have been taken both by state and non-state actors to combat this, however.

Relevant EU instruments

The EU has instruments in place that related to the consumers, targets, and vectors of disinformation. These include, in particular, the:

- East StratCom Task Force/EUvsDisinfo campaign;
- Western Balkans and South StratCom Task Forces;
- EU Code of conduct on countering illegal hate speech online;
- 2018 Action Plan Against Disinformation
- Rapid Alert System, set up among EU institutions and Member States to enable smooth data sharing and alerts on disinformation threats;
- the Code of Practice on Disinformation, signed by online platforms including Facebook, Google, and Twitter;
- 2020 European Democracy Action Plan;

- 2020 Digital Services Act;
- European Digital Media Observatory,
- European Parliament's Special Committee on Foreign Interference in all Democratic Processes in the EU (INGE).

The analysis of these initiatives shows, however, that what is lacking are instruments that would target those who deliberately produce and spread disinformation. Apart from that, it would be useful to consider how to also cover non-Russian disinformation players in a manner similar to EUvsDisinfo, and how to improve the coordination of the various initiatives and countermeasures against disinformation (e.g. via a new dedicated agency). The implementation of some of the instruments, e.g. RAS, could also be improved.

Lessons learnt for the EU

Based on the local lessons learnt through the case studies, the EU can draw the following lessons for its own work:

1) Disinformation actors use a wide range of channels, including seemingly independent websites and front media with no visible connection to the disinformation actors. External disinformers frequently use local actors and enablers to deliver their messages, or outsource activities to other countries.
2) Local nuances and polarisation of societies are key for understanding the disinformation environment.
3) There is significant disparity in resources between disinformation actors on the one hand, and civil society actors countering their activities on the other. Civil society actors lack resources to monitor, analyse, and counteract disinformation activities, and their work is made more difficult by domestic political actors utilising disinformation.
4) Research is missing on measuring the impact of disinformation activities, which can hinder civil society's efforts to counter disinformation.
5) Reliable media that effectively counter the disinformation-oriented "media" have a comparative disadvantage to the outlets focused on spreading disinformation.
6) Proactive campaigns pre-empting and neutralising disinformation in advance (using memes and humour) have proven to be effective in countering disinformation.
7) A whole-of-society approach to countering disinformation helps, but this is lacking in terms of limiting the effectiveness of counter-disinformation activities.

Recommendations for the EU

In order for the EU to be more effective at defending itself against malicious information operations, the following recommendations are proposed based on the lessons learnt:

- The European External Action Service (EEAS) and the Commission should introduce instruments similar to the EUvsDisinfo campaign aimed at detection and exposing of disinformation campaigns and raising awareness about them, also covering non-Russian disinformation players (e.g. China, Iran, or domestic EU actors).
- The European Commission should take action to ensure it more rapidly and robustly implements measures to support independent media and civil society initiatives countering disinformation within the EU. The EU could initiate the development of a new 'Transparency International for Disinformation', a dedicated CSO that regularly and systematically delivers comparable data about

disinformation campaigns from target countries to gain new and valuable data about the number of disinformation incidents, actors, vectors, channels, the success rate of disinformation, and relevant trends and development over time.

- The European Commission, the European Parliament, and the EU Member States should adopt measures that enable the perpetrators of disinformation to be punished and sanctioned, as envisaged in the European Democracy Action Plan (EDAP). This could entail sanctions against individuals and organisations regularly spreading disinformation, cutting them off from advertisement revenue and denying them access to EU institutions. To identify the individuals and organisations that should be sanctioned, the EU could consider launching official investigations into disinformation operations. Such investigations could be conducted at the EU level by special committees in the European Parliament, or by the EU Intelligence Analysis Centre (INTCEN) in the case of disinformation operations targeting the EU, and at the level of the Member States and local authorities (interior ministries, security services, national parliamentary committees) in case of disinformation operations targeting Member States.
- All European institutions and Member States should focus on developing rapid, proactive, pre-emptive campaigns based on real-time assessment of social media trends and topics identified as targets for disinformation campaigns, and ideally using humour.
- The EU should consider establishing a new EU agency for countering disinformation to better coordinate the EU's counter-disinformation initiatives. For better coordination between the EU and Member States, the EEAS should also motivate Member States to use the Rapid Alert System more effectively, and even consider opening this instrument to civil society alerts about disinformation incidents.

1 Introduction

1.1 Purpose and scope

The problem of disinformation and propaganda has continued to grow in recent years, constituting one of the most pressing threats for democratic countries. Data from 2019 showed a significant increase in global disinformation[1], and in 2020 this became a global infodemic. A lethal pandemic that ravaged the world in 2020 increased economic and physical insecurities worldwide, taking a toll on defenders of democracy. Authoritarian regimes, such as China or Iran, furthered their agendas under the guise of the pandemic, using disinformation as their tool of choice[2]. In 2020, Beijing intensified its global disinformation and censorship campaign to counter, distort, and hide the news of the initial COVID-19 outbreak from the world, hampering the global response to the threat[3]. A declassified National Security Council report revealed that while the United States (US) was holding Presidential elections in the middle of the COVID-19 pandemic, various Russian state and proxy actors were trying to influence US public opinion towards one candidate[4]. Iran also utilised the instability of 2020 and, through its proxies, wielded COVID-19 to bolster hostility in the Middle East against the US and its allies, while simultaneously building support for its own regime[5]. The actions of these countries added to overall global instability created by the pandemic. These challenges can be addressed, first and foremost, by understanding the disinformation methods and tactics used.

In this context, the European Parliament requested the current analysis to examine ways in which authoritarian regimes have used social media and other communication channels to influence public opinion and interfere in democratic processes. The goal is to increase understanding of such mechanisms by analysing specific examples; draw lessons from both the local and EU perspectives; and recommend ways in which the EU can improve its instruments and actions to respond to similar efforts of outside authoritarian regimes spreading messages within the EU.

To reach these goals, this paper focuses on three authoritarian regimes – Iran, China, and Russia – and their recent interference using social media platforms and other communication channels to target four selected information spaces. In the case of Iran, while the paper looks at its actions in the Middle East to some extent, it focuses in particular on Yemen and Syria. To examine Chinese interference, the paper analyses the experiences of Taiwan. To provide insight into the Russian misuse of social media and other communication channels, it zooms in on developments in Georgia. The main research questions that the case studies tackle are the following:

- In what way have the authoritarian regimes in Iran, China, and Russia misused social media and other communication channels to influence public opinion and interfere with democratic processes?
- What channels have been misused?
- Who has been involved in the misuse?
- Who has been targeted by the authoritarian regimes' misuse?

[1] Bradshaw, S., Bailey, H., Howard, P.N., Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation, University of Oxford, 2021.
[2] Whiskeyman, A,., Berger, M., Axis of Disinformation: Propaganda from Iran, Russian and China on COVID-19, Fikra Forum, 25 February 2021.
[3] Repucci, S., Slipowitz, A., Democracy under Siege, Freedom House, 2021.
[4] Polyakova, A., Fried, D., Democratic Offense Against Disinformation, CEPA, Atlantic Council, November 2020.
[5] Whiskeyman, A, Berger, M., op.cit.

- How have local governments and other actors responded to instances of misuse of social media and other communication channels?
- What lessons can be learnt from the experiences of those targeted by the authoritarian regimes' misuse?

Accordingly, the case studies describe examples of recent misuse and involve specification of the channels and methods applied by the respective regimes, as well as the measures adopted by authorities or other local actors in the places targeted to address interference and mitigate their impact.

While the paper focuses on the most recent developments in the context of foreign interference by the selected authoritarian regimes (including the COVID-19 pandemic), the analysis encompasses the period between 2015 and 2020.

The experiences studied are used to analyse and assess the EU external and internal policy instruments relevant for misuse of social media and other communication channels, particularly those focused on disinformation. In this respect, the paper considers how well these instruments would respond to the methods employed by external authoritarian regimes and whether the instruments are adapted to implement best practices, if and as revealed in the case studies. The paper then considers what the EU can learn from local experiences, and draws specific EU-level lessons which are coupled with recommendations for EU actors in various dimensions of EU actions.

In Section 1.2 we provide a brief overview of the concepts and definitions that are relevant for the study to further refine the scope. In Chapter 2, we succinctly summarise the international context, including recent research, to provide grounding for the subsequent case studies. In Chapter 3, we present the three selected case studies. For each of the case studies, analysis is structured into three sub-sections: (i) 'State of play', which outlines recent examples of the misuse of social media and other communication channels to influence public opinion and/or interfere in democratic processes; (ii) 'Response', which gives an overview of actions taken by governmental and/or non-governmental actors; and (iii) 'Conclusions and lessons learnt', where the analysis is summarised and specific local lessons are drawn. Chapter 4 provides an overview of the EU instruments relevant to this paper, as well as analysis and assessment of them in light of the case studies. In Chapter 5, we draw broader EU-level lessons, which are subsequently translated into specific recommendations presented in Chapter 6.

The analysis presented in the paper is based mainly on extensive desk research, encompassing both primary and secondary sources. The types of sources analysed included (i) academic literature; (ii) documents developed by EU institutions; (iii) documents and publications by international organisations and their bodies/mechanisms (e.g. bodies of the United Nations (UN), the Organization for Security and Cooperation in Europe (OSCE), the Council of Europe (CoE), etc.); (iv) grey literature by governments, think tanks, civil society organisations (CSOs) and international non-governmental organisations (INGOs), etc.; and (v) publications from established and independent media channels which display a high level of reporting. Additionally, a series of semi-structured interviews were conducted in August 2021 for the case studies. The interviews were conducted under the Chatham House rule, meaning that interviewees' comments were considered, but not attributed in this report.

1.2 Conceptual framework

The misuse of communication can be defined in various ways. We distinguish two main forms of the misuse of communication channels, namely (i) manipulation of content; and (ii) efforts to control the means of communication. A third manifestation would be a combination of the other two. Manipulation of content refers to methods for using information to influence public opinion. This can be further described with reference to the criteria for falseness and intent to harm (see Section 1.2.1). Efforts to control means of communication involve various ways of exerting influence over communication channels – for example

through financing, sponsoring, or in other ways supporting the activities of various actors carried out on communication channels. The proposed classification captures the three aspects which play a key role in spreading manipulated information: the methods used to manipulate the information, the media where the information is distributed, and the actors involved in its distribution.

1.2.1 Manipulation of content

For the purpose of this paper, we distinguish three types of manipulated content: disinformation, misinformation, and mal-information[6]. These are generally defined with reference to the criteria of falseness (or a misleading character) and intent to harm. Debate is ongoing around the exact meaning of these terms, with multiple definitions, typologies, and taxonomies having been proposed[7]. Whenever available, for the sake of coherence in our analysis and recommendations, we follow the definitions established in EU legal and policy frameworks, although these too are still developing[8].

Following the phrasing in the 2020 EDAP, we define disinformation as 'false or misleading content that is spread with intention to deceive or secure economic or political gain, and which may cause public harm'[9]. 'Public harm' is understood here as including 'threats to democratic political and policymaking processes, as well as public goods, such as the protection of EU citizens' health, the environment, or security'[10]. To put this in the simplest way possible, 'disinformation' is false or misleading information shared with intent to harm.

The 2020 EDAP also defines 'misinformation', and we adopt this definition for the paper. This form of misuse is thus understood as 'false or misleading content shared without harmful intent, though the effects can still be harmful (e.g. when people share false information with friends and family in good faith)'[11]. In short, misinformation is false or misleading information shared without intent to harm.

EU documents on disinformation do not offer a definition for mal-information. For the meaning of this term, we therefore refer to the conceptual framework developed for the CoE. We thus define mal-information as genuine information that is used to cause harm. This often involves the movement (or 'leaking') of information designed to stay private into the public sphere[12], which is a deliberate abuse of legitimate information by sharing it with the intent to harm. Mal-information can also include harassment or hate speech.

[6] We do not delve at length into 'propaganda'. As Jowett and O'Donnell define it, propaganda is a 'form of communication that attempts to achieve a response that furthers the desired intent of the propagandist'. Since this term does not necessarily reflect intent to harm, nor a false or misleading nature to the information, we generally prefer the use of other terms in this paper.

[7] See e.g. the conceptual framework proposed in Wardle, C., Derakhshan, H., Information Disorder. Towards and interdisciplinary framework for research and policymaking, Council of Europe, 2017. For a review of taxonomies and typologies, see e.g. Kapantai E, Christopoulou A, Berberidis C, Peristeras V., 'A systematic literature review on disinformation: Toward a unified taxonomical framework', New Media & Society, Vol. 23(5):1301-1326, 2020.

[8] e.g. recently, the EEAS submitted a non-paper to EP's INGE committee in which it notes a need for more 'refined common definitions and methodologies'. It proposes the term 'foreign information manipulation and interference' (FIMI) as a more accurately capturing the issue at stake, defining it as 'a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory'. See, EEAS, Foreign information manipulation and interference – creating a common basis for action, 2021.

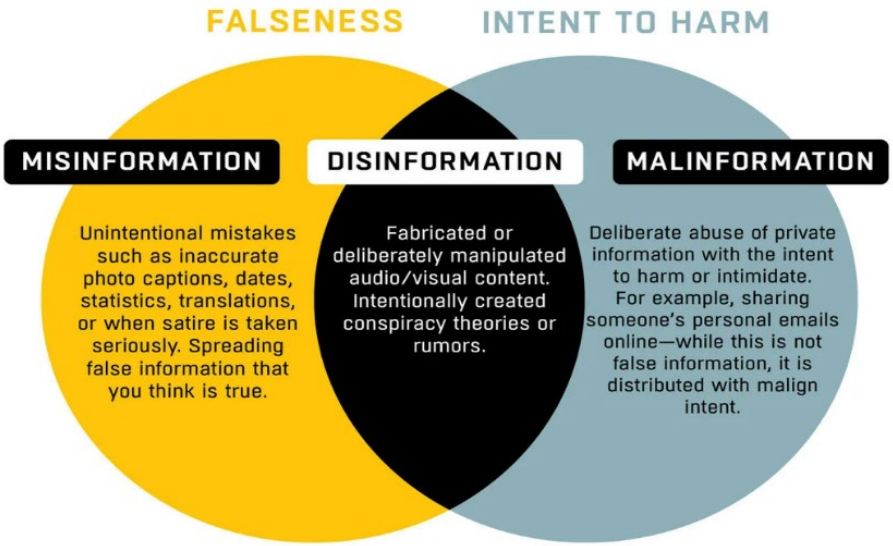
[9] European Commission, Communication for the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: On the European democracy action plan, COM(2020)790 final, 2020.

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

[11] COM(2020)790 final, 2020.

[12] Wardle, C., Derakhshan, H. INFORMATION DISRODER: Toward and interdisciplinary framework for research and policy making, Council of Europe report DGI(2017)09, 2017.

Figure 1: Interaction between the three main types of manipulation (misinformation, disinformation, and mal-information).



Source: Verified.ed-era.com

In our subsequent analysis of case studies and EU instruments, we focus primarily on disinformation. On the one hand, this allows us to deepen the analysis of disinformation itself. On the other, since the phenomenon entails both falsehood and intent to harm, it means that we cover the most serious manifestation of content manipulation. While beneficial for deepening reflection, this focus is also relevant from the perspective of recommendations. The countermeasures to disinformation would fall under external policy, as opposed to misinformation, for example, which would mostly be tackled 'from the perspective of home affairs and the health of public debate', falling into the remit of Directorates-General (DGs) such as Justice and Consumers (JUST), Communications Networks, Content and Technology (CNCT), Education, Youth, Sport and Culture (EAC), and Communication (COMM)[13]. Nevertheless, while disinformation has been the main focus, misinformation and mal-information have also been covered wherever relevant.

1.2.2 Efforts to control the means of communication

Efforts to control the means of communication can be made, for example through funding the activities of various actors.

In terms of funding, efforts to control means of communication can take the form of ownership or backing of media outlets. Authoritarian regimes may partially or fully own media outlets while exerting control over their editorial content. An example of a state-backed, partially state-owned outlet is the Russian RT.com, while a fully 'state-owned media outlet' (publicly known or unknown information)[14] is RIA Novosti[15]. States can also fund or otherwise support (reporting by) media outlets they do not own. These outlets may be mainstream (i.e. media that influence large numbers of people and are likely to represent generally

[13] Pamment, J., The EU's role in fighting disinformation: Crafting a new disinformation framework, Carnegie Endowment for International Peace Working Paper, 2020.
[14] Lucas, E., Morris, J., Rebegea, C., Information Bedlam: Russian and Chinese Information Operations During Covid-19, CEPA, March 15, 2021.
[15] Ibid.

accepted beliefs and opinions) or 'fringe' (those with more limited distribution, followers, subscribers, or journalistic quality). An example of a fringe source would be 'The Baltic Word' website, which focuses on spreading Baltic-related disinformation.

Authoritarian regimes can make recourse to an array of different actors who serve as proxies or multipliers of their messages, hijacking the debate (e.g. trolls, bots, and sock-puppets)[16]. According to the DFRLab, a 'troll' is an account run by a human which systematically posts inflammatory, divisive, or abusive content with the goal of provoking. Trolls often work under a cover of anonymity[17]. A 'bot' is an inauthentic account run by an algorithm that is able to spread content without constant human observation or effort[18]. Lastly, a 'sock puppet' is an online account run by a human pretending to be someone else in order to trick their followers[19].

[16] Associated Press, Cyborgs, Trolls and Bots: A Guide to Online Misinformation, VOA News, 8 February, 2020.
[17] Donara Barojan, #TrollTracker: Bots, Botnets, and Trolls, DFRLab, 09 October, 2018.
[18] Ibid.
[19] Kaul, A., Sockpuppet accounts impersonate India's space agency chief, DFRLab, 18 November, 2019.

2 The current state of play and overview of research

In recent years, much research has been done on different forms of misusing social media and other communication channels[20], the spread of manipulated content[21] and the ways to counter these phenomena[22]. Researchers have examined the activities of authoritarian regimes outside their own borders, and have shown that the COVID-19 pandemic has intensified some regimes' malpractices, contributing further to the deterioration of democratic standards and freedom in the world[23].

The use of social media to hijack a trend can make the spread of disinformation faster and easier than ever before[24]. While data show that authoritarian regimes are not the only actors involved in manipulating content, they have been able to leverage the specific features of social media to their advantage[25]. After initially pursuing an approach of *information scarcity* with censorship and restrictions on access, they now also embrace *information abundance*[26]. As Jones notes, '[t]he window that social media provided for challenging authoritarian control of the media was short-lived, having since been co-opted mainly as a tool of repression and disinformation'[27].

In a 2020 study, scholars presented a dataset encompassing 76 foreign influence efforts (FIEs) initiated by a state or the ruling party in an autocracy carried out in 30 countries[28]. Within the dataset, Russia was the main country behind FIEs, peaking in 2017 with involvement in 34 distinct campaigns. Other countries that initiated FIEs during the study period included China, Egypt, Iran, Saudi Arabia, United Arab Emirates and Venezuela. The authors found that 'Iran was involved in two cases between 2014 and 2015, but steadily increased their activity through 2018 when they were operating against 10 other nations'[29]. Similarly, an earlier, 2018 study found that 'interlocutors among European authorities attribute 80 % of influence efforts in Europe to Russia', with the remainder being split between state actors such as China and Iran, as well as non-state actors, including Jihadist groups such as ISIS[30]. In its 2020 summary on disinformation, Brookings reported that 'Facebook and Twitter most frequently attributed foreign influence campaigns to actors in

[20] Including at the initiative of the European Parliament: Bayer, J. et al., Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, European Parliament, 2019; Bayer, J. et al., Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States. 2021 update, European Parliament, 2021; Greene, S., Asmolov, G., Fagan, A., Fridman, O., Gjuzelov, B., Mapping Fake News and Disinformation in the Western Balkans and Identifying Ways to Effectively Counter Them, European Parliament, 2020.

[21] See e.g. Starbird, K., Disinformation's spread: bots, trolls and all of us, Nature, 24 July, 2019; Guess, A., Nagler, J., Tucker, J., Less than you think: Prevalence and predictors of fake news dissemination on Facebook, Science Advances 5, eaau4586, 2019; Grinberg, N. et al., Fake news on Twitter during the 2016 U.S. presidential election, Science, Vol 363, Issue 6425, pp. 374-378, 2019; Shao, C., Ciampaglia, G.L., Varol, O. et al., The spread of low-credibility content by social bots, Nature Communications 9, 4787, 2018; Vosoughi, S., Roy, D., Aral, S., The spread of true and false news online, Science, Vol. 359, Issue 6380, pp.1146-1151, 2018.

[22] Helmus, T.C., Kepe, M., A Compendium of Recommendations for Countering Russian and Other State-Sponsored Propaganda, Rand Corporation, 2021. The compendium presents the results of a review encompassing 64 policy reports on countering Russian and other state-sponsored propaganda which contained separate sections related to recommendations.

[23] Repucci, S., Slipowitz, A., Democracy under Siege, Freedom House, 2021. See also, Bayer, J. et al., 2021.

[24] Prier, J., Commanding the Trend: Social Media as Information Warfare, Strategic Studies Quarterly, 11 (4), 2017.

[25] Such as aggregation, algorithms, anonymity and automation (automated accounts). See Bradshaw, S., Influence Operations and Disinformation on Social Media, Centre for International Governance Innovation, 23 November 2020.

[26] Nyst, C., Monaco, N., State-sponsored Trolling, How governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns, Institute for the Future Digital Intelligence Lab, 2018.

[27] Jones, M.O, Disinformation super-spreaders: the weaponisation of COVID-19 fake news in the Persian Gulf and beyond, Global Discourse, vol 10, no 4, 431–437, 2020.

[28] Importantly, influence efforts are defined here as: '(i) coordinated campaigns by a state or the ruling party in an autocracy to impact one or more specific aspects of politics at home or in another state, (ii) through media channels, including social media, by (iii) producing content designed to appear indigenous to the target state.' Martin, D.A., Shapiro, J.N., Ilhardt, J.G., Tracking Online Influence Efforts, 1 November, 2020.

[29] Ibid.

[30] 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, Paris, August 2018.

Russia, Iran, and Egypt', and the same countries carried out foreign operations in 2019 according to the authors' own dataset[31].

Reflecting their engagement in content manipulation through social media and other communication channels worldwide, Russia and China have received significantly more attention in research, which has also largely focused on the U.S. and Europe as targets[32]. In some of the more recent research, in the study "Bringing Psychological Operations and Military Information Support Operations into the Joint Force: Counterinformation Campaigns in the Social Media Age", Rand has produced four reports in the Combating Foreign Disinformation on Social Media Series. In addition to an overview report[33] and a report on the U.S. efforts to combat foreign disinformation[34], these included two reports exploring Chinese[35] and Russian[36] disinformation efforts. Regular research and reporting on these countries has been provided by think tanks (such as e.g. the Atlantic Council's Digital Forensic Lab[37]) or CSOs (e.g. Freedom House[38]).

Think tanks and CSOs have also developed tools to track authoritarian interference by the most active authoritarian regimes. For example, the Alliance for Securing Democracy has developed the Authoritarian Interference Tracker which catalogues the Russian and Chinese governments' activities in employing tools such as information manipulation and cyber operations, among others, to undermine democracy in over 40 countries since 2000[39]. The organisation has also developed the Hamilton 2.0 dashboard which provides 'a summary analysis of the narratives and topics promoted by Russian, Chinese, and Iranian government officials and state-funded media on Twitter, YouTube, state-sponsored news websites, etc.[40]

Until recently, researchers focused largely on Russia which has become expert in applying the experience of the Soviet era in manipulating information to the new digital media landscape[41]. Researchers have, for example, studied the tsunami of well-conceived and targeted disinformation by Russia around the annexation of Crimea[42]. As Stengel writes, the world had not seen such 'startling Russian fiction since Dostoyevsky'[43]. Information disseminated by pro-Kremlin media presented Russian forces in Crimea as 'citizens' defence groups' acting to protect Russian military assets and Russian minorities, when in reality the troops were Russian military forces who seized the infrastructure and military facilities in Crimea with the aim of annexing its territory[44]. Even more than Moscow's disinformation about Crimea, its interference in the U.S. 2016 elections has been the most researched recent case, also deemed a 'turning point in the use of online information campaigns'[45].

Various actors have tried to monitor and analyse Russia's misuse of social media and other communication channels. In the EU, investigation of Russian disinformation is the central focus of the EUvsDisinfo campaign conducted by the EEAS's East StratCom Task Force. In addition to maintaining its database of

[31] Goldstein, J.A., Grossman, S., How disinformation evolved in 2020, 4 January, 2021.
[32] Jones, M.O., op. cit., 2020.
[33] Cohen, R.S. et al., Combating Foreign Disinformation on Social Media: Study Overview and Conclusions, RAND Corporation, 2021.
[34] Cohen, R. S., Demus, A., Schwille, M., Vest, N., U.S. Efforts to Combat Foreign Disinformation on Social Media, RAND Corporation, 2021, not available to the general public.
[35] Harold, S.W., Beauchamp-Mustafanga, N., Hornung, J.W., Chinese Disinformation efforts on social media, Rand Corporation, 2021.
[36] Treyger, E., Cheravitch, J., Cohen, R.S. (n.d.), Russian Disinformation Efforts on Social Media, RAND Corporation, forthcoming.
[37] Available at: www.digitalsherlocks.org/ourwork and https://medium.com/dfrlab
[38] Available at: https://freedomhouse.org/expert/sarah-cook
[39] Available at: https://securingdemocracy.gmfus.org/toolbox/authoritarian-interference-tracker/
[40] Available at: https://securingdemocracy.gmfus.org/hamilton-dashboard/
[41] The Council's library has, for example, compiled a list of reading references on Soviet and Russian disinformation.
[42] Stengel, R., Information Wars: How We Lost the Global Battle Against Disinformation and What We Can Do About It, *Atlantic Monthly Press*, 2019.
[43] Ibid.
[44] Ibid.
[45] Rob, J.T., Shapiro, J.N., A Brief History of Online Influence Operations, Lawfare Blog, 28 October, 2021.

campaigns, producing own analysis and reviews, including on the COVID-19 related disinformation[46], the East StratCom maintains a compilation of various sources relating to pro-Kremlin disinformation[47].

While research shows that Russia has supported specific political actors worldwide, Martin et al. note that '[r]ather than following a fixed political ideology, Russian FIEs sometimes focus on stoking social tensions or pragmatically adjusting support according to different geopolitical goals'[48]. One of the foci of the Kremlin regime has been influencing foreign elections[49]. As the EEAS has documented, the Russian toolbox for meddling in elections includes disinformation, political advertising, sentiment amplification, identity falsification, hack-and-leak operations and reconnaissance hacking, among others[50].

Moscow has used a plethora of vehicles to further its agenda. State-owned or state-backed media outlets have pursued Russia's interests also by means of disinformation and propaganda. All Russian mainstream media are either owned by the state or other actors tied to the state, such as a state company or an oligarch close to the government[51]. RT (previously Russia Today) has been Russia's disinformation flagship and 'one of the most important organisations in the global political economy of disinformation[52].

Apart from taking ownership of media outlets (by buying out or taking over existing outlets by force and creating new ones), Russia has used private actors with 'troll farms' or 'cyber troops', such as the 'Internet Research Agency'[53]. Other such actors working for authoritarian regimes include China's '50 Cent Army'[54], and Turkey's 'AK Trolls'[55]. Their main task is to spread different messages, targeting wide audiences, in order to achieve a particular goal, while masquerading as authentic users or commentators on mainstream social media[56]. Even though researchers were able to spot foreign trolls with relative ease since the phenomenon started, foreign trolls have now become much more sophisticated, and therefore harder to notice[57]. As observed by Lt Col Jarred Prier, Russian trolls have a wide variety of state resources at their disposal, including a vast intelligence network to assist their cyber warriors[58]. Analysts also note the activities of 'Potemkin personas'[59] (aka 'sock-puppet' accounts), i.e. foreign trolls who build a credible online presence across multiple platforms and mix their political messaging with banal posts about their supposed daily life, much like an authentic user would do. This includes creating fake personas that pose as experts, writers, or journalists[60].

The Kremlin has also exerted its influence through ensuring control over other countries' media sectors. In 2018, the Centre for the Study of Democracy (CSD) investigated Russian influence in the media sectors of the Black Sea countries, confirming that 'the patterns of ownership, economic dependency and (in)formal

[46] Available at: https://euvsdisinfo.eu/category/blog/eeas-special-reports/
[47] Available at: https://euvsdisinfo.eu/reading-list/
[48] Martin, D.A., Shapiro, J.N., Ilhardt, J.G., op. cit., 2020.
[49] Tennis, M., Russia Ramps up Global Elections Interference: Lessons for the United States, Centre for Strategic & International Studies, 2020.
[50] Available at: https://euvsdisinfo.eu/methods-of-foreign-electoral-interference/
[51] Meister, S. et al., Understanding Russian Communication Strategy: Case Studies of Serbia and Estonia, 2018.
[52] Elswah, M., Howard, P.N., "Anything that Causes Chaos": The Organizational Behavior of Russia Today (RT), Journal of Communication, Volume 70, Issue 5, October, 2020.
[53] Dawson, A., Innes, M. How Russia's Internet Research Agency Built Its Disinformation Campaign, The Political Quarterly, Vol. 90, No. 2, 2019.
[54] King, G., Pan, J., Roberts, M.E., How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument, American Political Science Review, Vol. 111, No. 3, August 2017.
[55] Bulut, E., Yörük, E., Mediatized Populisms | Digital Populism: Trolls and Political Polarization of Twitter in Turkey, *International Journal of Communication*, Vol. 11, 2017.
[56] Ben Nimmo, #BotSpot: Twelve Ways to Spot a Bot, DFRLab, 29 August, 2017.
[57] Bayer, J. et al., op. cit., 2021.
[58] Prier, J. Commanding the Trend: Social Media as Information Warfare, Strategic Studies Quarterly, 11 (4), 2017.
[59] Diresta, R., Grossman, S., 'Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019', Cyber Policy Center, 2019.
[60] Ibid. See also, Jones, M.O, op.cit., 2020.

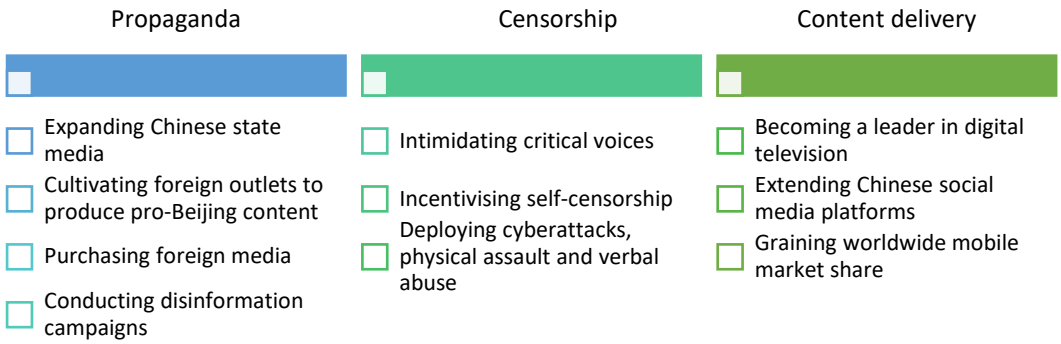
political links of media outlets in the countries under investigation to pro-Russian groups and interests are correlated with and reflected into corresponding trends of employing Russia-originating propaganda narratives'[61]. In its recent studies, CSD analysed Russian media capture in Southeast Europe and revealed 'the increasing overlap of influence tactics between Russia and other authoritarian states operating in the Balkans, particularly China'[62].

The Chinese Communist Party is currently catching up when it comes to the misuse of social media and other communication channels[63], including in its effort to counter the negative implications of the COVID-19 pandemic on its image[64]. Some of the more studied cases include China's interference in Taiwan[65] or Hong Kong. Additionally, while occasional links between Russia- and Iran-related propaganda sources were observed before the pandemic, the COVID-19 crisis has apparently contributed to greater alignment between disinformation coming from these countries and the PRC, prompting Andrew Whiskeyman and Michael Berger to call them an 'Axis of Disinformation'[66]. Since the COVID-19 outbreak, 'China has begun to overtly amplify and shape the disinformation narratives, following the release of Russian and pro-Iranian propaganda'[67]. While Chinese, Russian and Iranian messages have so far converged on a limited number of arguments – in particular, that the US is responsible for COVID-19 – the coordination may evolve to cover more topics.

As Chinese engagement in the misuse of social media and other communication channels intensifies, so does the attention of researchers. In a 2020 special report, Freedom House's Sarah Cook comprehensively analyses the expansion of Chinese Communist Party (CCP) media influence since 2017, tackling its goals, means and tactics, impact and pushback[68]. As Cook observes, aside from traditional goals of promoting a positive Chinese story, investment and supressing criticism, in recent years Chinese media influence campaigns also attempted to present 'China's authoritarian style of governance as a model for developing countries to emulate'[69], while undermining democratic governance and US leadership. As is the case with Russia, the Chinese toolbox of 'censorship, propaganda and control over content-delivery systems extends beyond the borders of mainland China', comprising a plethora of tactics (see Figure 2).

[61] Filipova, R., Galev, T., Russian Influence in the Media Sectors of the Black Sea Countries. Tools, Narratives and Policy Options for Building Resilience, Centre for the study of Democracy, 2018. See also another recent study by CSD: Filipova, R., Stefanov, R., Countering Kremlin's Media Influence in Europe, Patterns of Anti-Democratic Messaging, Disinformation Responses, and Resilience Assets, Centre for the Study of Democracy, 2021.
[62] Filipova, R., Vladimirov, M., Gerganov, A., Tackling Kremlin's Media Capture in Southeast Europe. Shared patters, specific vulnerabilities and responses to Russian disinformation, Centre for the Study of Democracy, 2021.
[63] Roberts, D., China's disinformation strategy. It's dimensions and future, Atlantic Council, The Scowcroft Centre for Strategy and Security & The Digital Forensic Research Lab, 2020.
[64] Repucci, S., Slipowitz, A., op. cit., 2021.
[65] Apart from the case study in this paper, see also Bayer, J. et al., op. cit., 2021.
[66] Whiskeyman, A., Berger, M., 'Axis of Disinformation: Propaganda from Iran, Russia, and China on COVID-19', The Washington Institute for New East Policy, 2021.
[67] Ibid.
[68] Cook, S., Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence since 2017, Special Report, Freedom House, 2020.
[69] Ibid.

Figure 2: Based on the graphic 'China's Toolbox for Global Media Influence' in Cook, S, Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence since 2017, Special Report, Freedom House, 2020.



Cook describes how, with substantial financial investments, China is expanding the reach of its state-owned media outlets worldwide by increasing their presence on popular social media platforms, using both soft content and misleading advertising. While Beijing makes frequent use of legitimate public diplomacy, the more ambiguous tactics include inserting paid news-like advertising in the print editions of newspapers (noted e.g. in the US, Spain, the UK, Australia, Argentina, Peru, Senegal and India) and signing news exchange agreements between Chinese agencies such as Xinhua and partner media around the globe. Xinhua agency has reportedly signed cooperation pacts in countries including Australia, Italy, Bangladesh, India, Nigeria, Egypt, Thailand,[70] Vietnam, Belarus, and Laos. Sometimes Chinese actors coproduce content with local actors or use favourable local actors (e.g. journalists or media tycoons) to produce content that serves its goals.

Cook also describes how the use of China's Russian-style disinformation campaigns on international social media platforms has gained prominence over the past years. She discerns characteristic features of those disinformation efforts, including: (i) much of the content being in Chinese, suggesting a focus on the diaspora; (ii) the use of accounts bought on the black market; (iii) less psychological sophistication and more haste in deployment, as compared to Moscow's effort during the 2016 U.S. elections, particularly in terms of meaningful engagement with local users[71]. The study by the Alliance for Securing Democracy has in turn shown how China-related actors (e.g. officials and media) are exploiting gaps in search results (the so-called data voids) on search engines such as Google, YouTube and Bing to spread conspiracy theories related to COVID-19 origins[72].

Other tactics that China has employed included: (i) China-linked actors' purchasing full or partial ownership stakes in media outlets, bringing changes in editorial policy in reporting; (ii) involvement of Chinese companies in transitions from analogue to digital television broadcasting, especially in Africa[73]; (iii) expanding the reach of social media firms, such as WeChat by Tencent or TikTok developed by the ByteDance, reportedly accompanied by content monitoring and censorship on the applications, including enforcing self-censorship; (iv) seizing the mobile device markets as a way to gain influence over communication[74]. As Cook notes, 'to date, there has been no systematic research or testing of censorship

[70] See also, Gershaneck, K.K., Political Warfare. Strategies for Combating China's Plan to "Win without Fighting", Marine Corps University Press, Quantico, Virginia, 2020.
[71] Cook, S., op. cit. 2020.
[72] Aghekyan, E., Schafer, B., Deep in the Data Void: China's COVID-19 Disinformation Dominates Search Engine Results, Alliance for Securing Democracy, 5 October, 2021.
[73] Outside of Africa, for example, Huawei led the transition from analogue to digital television in Cuba, Pakistan, Laos, Cambodia and Timor-Leste. Cook, S., op. cit. 2020..
[74] Ibid.

on the browsers of Chinese-made smartphones, so it is difficult to know whether and how many hurdles are being placed in the way of global users'[75]. However, as she underlines, 'Chinese companies' growing role in content delivery systems creates opportunities for the CCP to influence not only foreigners' views about China but also the news they receive about their own countries and political leaders, with possible implications for the outcome of elections'[76].

In a more recent, 2021 paper, Cook expands on the China's global media footprint, while zooming in on the democratic responses to expanding authoritarian influence[77]. She provides ample examples of actions taken in response by non-governmental actors such as media, think tanks, civil society and tech companies. These responses include discontinuing paid advertorials, pushing back collectively, exposing influence efforts, submitting complaints, labelling media, discontinuing advertising, and more.

[75] Ibid.
[76] Ibid.
[77] Cook, S., China's Global Media Footprint. Democratic responses to expanding Authoritarian Influence, Sharp Power and Democratior Resilience Series, National Endowment for Democracy, 2021.

3 Examples of foreign interference outside the EU

This chapter presents case studies of three authoritarian regimes and their interventions. In the case of Iran, the choice of targeted countries was dictated by the intensity of regimes' actions in the area, while analysis of China and Russia was explicitly requested by the European Parliament. Each case study was conducted based on desk research and semi-structured interviews with journalists, activists and local representatives of CSOs.

3.1 Iran's interventions in the Middle East

Since the formation of the Islamic Republic in 1979, the Iranian foreign policy of "exporting the revolution" has guided Iran's information influence operations. These measures continue to evolve with advancements in media and communication technologies[78], making Iran one of the most prolific purveyors of disinformation and mal-information in the Middle East. Iran's weaponisation of social media is part of a broader scheme for influence in states with strategic value to the nation's foreign policy. Its information activities occur in tandem with media broadcasting, on-the-ground promotional activities, recruiting of Shi'a minorities on an ideological basis, and supporting business operations for post-war reconstruction in countries like Syria. Iran's information influence operations through social media are an indicator of how it pursues its national interests and foreign policy priorities. These operations often propagate pro-Iran narratives through front media and their social media platforms to maximise reach. Since 2018, Facebook and Twitter have suspended multiple networks of Iran-affiliated accounts. Countering the narratives that Iran systematically promotes in Yemen and Syria requires comprehensive multi-stakeholder efforts that tackle different aspects of these activities, however.

3.1.1 State of play

In addition to transnational networks such as Al-Alam, an Arabic-language channel that receives support from the Islamic Revolutionary Guard Corps (IRGC)[79], Iran has utilised the Islamic Radio and Television Union (IRTU), a body affiliated with the Ministry of Culture and Islamic Guidance that has an extensive network of subsidiaries that use traditional broadcasting in tandem with social media for enhanced reach[80].

Takedowns of information influence operations disclosed by social media platforms since 2018 portray Iran as the most prolific actor in the Middle East and North Africa (MENA) [81]. Between August 2018 and March 2021, 46 information operations originating from 10 MENA countries were removed by Facebook and Twitter. As many as 20 out of 46 datasets had originated from Iran[82]. Conflicts in Yemen and Syria remain core to Iran's foreign policy, a priority that is also reflected in many of Iran's information influence operations. The greatest number of websites that FireEye[83], Reuters[84], and ClearSky[85] attributed to Iran in 2018 targeted audiences in Yemen and Syria[86]. Since then, a growing number of Iran-affiliated accounts have been suspended by social media companies[87]. In addition, since October 2020, the US Department of

[78] Anderson, C., Sadjadpour K., Iran's Cyber Threat: Espionage, Sabotage, and Revenge, Carnegie Endowment for International Peace, 2018.
[79] Torfeh, M., The Role of Iran's Regional Media in its Soft War Policy, Al Jazeera Center for Studies, 2017.
[80] Iranwire Arabic, Learn About The Islamic Radio And Television Union, Which Washington Closed Most Of Its Media Outlets, 2021.
[81] DiResta, R., Goldstein, J., Grossman, S., Middle East Influence Operations: Observations Across Social Media Takedowns, Project on Middle East Political Science (POMEPS), 2021.
[82] Ibid.
[83] FireEye, Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East, 2018.
[84] Stubbs, J., Bing, C., Special Report: How Iran spreads disinformation around the world, Reuters, 2018.
[85] ClearSky, Global Iranian Disinformation Operation, 2018.
[86] Swanbeck, S., How to Understand Iranian Information Operations, Lawfare, 2021.
[87] See for example Twitter Blog, Disclosing networks of state-linked information operations, 2021.

Justice has seized an extensive network of Internet domains linked to the government of Iran for spreading false information around the world[88].

Much of Iran's disinformation focuses on casting the Iranian government and its anti-Western ideology and regional strategic interests in a positive light. In doing so, Iran seeks to demonise its adversaries (e.g. the US and Israel) and regional rivals (e.g. Saudi Arabia and the United Arab Emirates (UAE)) to the foreign general public. Not only does Iran attempt to influence domestic affairs and foreign relations in rival countries[89], but it also bolsters proxy groups and pro-Shi'a narratives in Yemen and Syria – both torn by conflicts that Iran has played a key role in. In Yemen, many of these activities are directed toward bolstering narratives in favour of the Houthi movement, a militant Zaidi-Shi'a movement officially known as 'Ansar Allah'[90]. Iran has backed the Houthis in the Yemen civil war since 2015[91].

Iran pursues these objectives through a variety of tactics. Chief among them is 'laundering propaganda'[92] through front and proxies' media (e.g. Al-Masirah in Yemen and Al-Jeish in Syria). These outlets selectively re-publish articles from state or state-affiliated media, and are ideologically aligned with the Islamic Republic. Others impersonate real news sites, re-posting some original content to appear more legitimate. These outlets often use standard newspaper naming conventions, such as 'Yemen Press' and 'Daily Syria News'[93], and obscure domain registration information in order to evade attribution. Both groups utilise Facebook, Instagram, Twitter, and YouTube to enhance their reach and engagement.

Iran is also looking to professionalise disinformation beyond its borders. It has moved toward outsourcing disinformation to regional proxies to expand the reach and efficacy of these activities. Hezbollah, for example, has stepped up to run 'disinformation bootcamps' in Lebanon to train transnational, Iran-backed social media activists[94]. They have recruited trainees from several MENA countries, including Syria, and equipped them with the skills required to manipulate public discourse on social media platforms[95].

3.1.2 Targets of Iran's mal-information in the region

Identifying the targets of information influence operations is not so straightforward. Iran's sprawling media apparatus, in particular Al-Alam TV and its franchises, broadly target Shia Arabs across the Middle East, seeking to diminish the influence of Iran's Sunni rivals in the region[96]. A great number of Iran-associated media specifically cater to local audiences (e.g. Al-Hawyah and Al-Sahat in Yemen), seeking to promote narratives in favour of Iran's strategic interests in these countries. There is also a third group of outlets with a more nuanced approach. Several now-defunct news sites purporting to run from Yemen propagated Iranian narratives about Syria[97]. Others attempted to impress Arabic-speaking audiences, regardless of their location or demographics, with Syrian history and culture, while promoting a pro-Assad rhetoric[98]. Such diverse tactics illustrate Iran's 'kitchen sink' approach to engaging a broad spectrum of audiences though social media and other communication channels that may yield strategic gain. However, these information influence operations are but one avenue for influencing the public's perception of Iran's

[88] U.S. Department of Justice, United States Seizes Domain Names Used by Iran's Islamic Revolutionary Guard Corps, 2020.
[89] DiResta, R., Goldstein, J., Grossman, S., op. cit.
[90] Khalaji, M., Yemen's Zaidis: A Window for Iranian Influence, The Washington Institute for Near East Policy, 2015.
[91] Juneau, T., How Iran Helped Houthis Expand Their Reach, War on the Rocks, 2021.
[92] DFRLab, #TrollTracker: Twitter Troll Farm Archives; Part Three — Assessing an covert Iranian social media influence campaign, 2018.
[93] ClearSky, Global Iranian Disinformation Operation.
[94] Levitt, M., Hezbollah's Regional Activities in Support of Iran's Proxy Networks, Middle East Institute, 2021.
[95] Telegraph, Exclusive: Inside Hizbollah's fake news training camps sowing instability across the Middle East, 2020.
[96] Siegel, A., Official Foreign Influence Operations: International Broadcasters in the Arab Online Sphere, POMEPS, 2021.
[97] For example, the allegedly Yemen-based news site 'al-mersad.com' used to promote pro-Iran narratives with regards to the conflict in Syria. Available at: https://web.archive.org/web/20130402175116/http://al-mersad.com/.
[98] See for example an archived version of Syria Blog at: https://web.archive.org/web/20140228060714/http://syria-blog.com/.

intentions in countries like Yemen and Syria. As one interviewee explained[99], in addition to its information influence operations, Iran seeks to expand its extraterritorial network of supporters by tending to particular demographics, such as the Shi'a tribes in Syria. Through a combination of financial interventions, mostly in favour of Shi'a minorities, and information influence operations, Iran seeks to propagate narratives that bolster its geopolitical objectives, erode trust in media and local authorities, and sow chaos in the region.

3.1.3 Local responses to information pollution

Counter-responses to Iran's disinformation have been limited in number and scope. Limited government capacity in Yemen and geopolitical circumstances in Syria have reduced the possibility of any state initiatives in either county. The disparity of resources between civil society and Iran's propaganda apparatus perpetuate the lack of factually sound information.

According to one interviewee[100], the ongoing crisis in Yemen has caused an 'information fatigue' among the public, creating a crisis of trust in media, authorities, and international actors. The media is generally perceived as biased toward one side or the other, highlighting the need for independent coverage and analysis. The vacuum of credible information perpetuates the circumstances that the Houthi movement has thus far utilised in favour of Iran.

A number of civil society initiatives have sought to fill in the gap with fact-based information. 'Yemeni Archive', an CSO, documents human rights violations and other war crimes committed by all parties in Yemen for advocacy and accountability purposes. 'Mwatana for Human Rights', another CSO, documents human rights violations by all parties to the conflict, provides legal support to the victims, and conducts research and advocacy. The two Yemeni interviewees that we spoke to view these efforts as non-mainstream with limited influence on public opinion, but emphasised that the existence and promotion of such initiatives is an important step in the right direction.

In Syria, few fact-checking initiatives or investigative journalism projects have existed thus far. While there is a dire need for such an initiative in Syria, the number of existing projects on investigative journalism are far behind the still-growing (and less than optimal) figures of global initiatives. As one interviewee observed, Syrian Investigative Reporting for Accountability in Journalism (SIRAJ) is the first Syrian initiative that seeks to equip journalists with investigative tools[101]. According to the interviewee, training journalists who can pass on acquired skills to others is a lengthy process, and requires significant investment in terms of time and resources, with returns that may not be immediately measurable. Together with the typically limited duration of funding engagements, these challenges undermine the sustainability of investigative initiatives in the long run.

Another key challenge, as our interviewees described, is communicating reliable information to the outside world according to the highest fact-checking standards, without compromising the identity of sources. Security concerns complicate trust building between diaspora fact-checkers and local collaborators who can help with verification of primary information[102]. According to a Yemeni scholar who requested anonymity for security reasons, preserving the digital security of fact checkers and their local network is an area that needs constant attention and improvement.

[99] The interview was conducted during the course of this study on August 27, 2021.
[100] The interview was conducted during the course of this study on August 26, 2021.
[101] The interview was conducted during the course of this study on August 27, 2021.
[102] The interview was conducted during the course of this study on August 27, 2021.

3.1.4 Conclusions and lessons learnt

Iran has created a sprawling apparatus that seeks to influence public opinion in many states, including Syria and Yemen, to build soft power and combat its regional rivals' authority (particularly Saudi Arabia). Iranian information influence operations often serve as a means of public relations, rather than an end. They are aimed at drawing attention to geostrategic narratives, rather than engaging with the audience on an individual level (for example, through hashtags like #NoWarInYemen to illustrate regional tensions). Yet these activities remain covert in nature due to their use of apparently independent websites and accounts to promote Iran's narratives[103]. Responses to Iran's disinformation have been limited in number and scope. With state reactions hindered by insufficient capacity, the geopolitical situation, or a general climate of distrust towards the media, some civil society initiatives have focused on documentation or fact-checking.

In light of the analysis, the following specific lessons can be learnt:

1) Iran's information influence operations in Syria and Yemen highlight the importance of persistent monitoring of the technical infrastructure and social media debates that weaponise regional tensions to amplify Iran's interests. Technical tools and discourse analysis platforms are key to understanding the evolving infrastructure of Iran's front media and their discursive tactics.

2) Countering Iran's disinformation is partly a matter of internet governance. Formulating effective policy responses in this space requires multi-stakeholder engagement and longitudinal evaluation. In the past, the U.S. Department of Justice has seized generic Top-Level Domains (gTLD, such as .com and .net), which may limit the reach of disinformation activities by Iran and its proxies to some extent. However, the Houthis have seized control over the country code Top-Level Domain (ccTLD) for Yemen (.ye), which enables them to replace suspended gTLDs with Houthi-controlled '.ye' domains[104]. These local and global power dynamics of internet governance complicate counter responses to Iran's influence in online spaces.

3) Tracking the role of key purveyors of Iran's disinformation across the region, such as Hezbollah and the Houthis, is paramount to mapping the broader landscape of Iran's information influence operations. As Iran mobilises more local and regional players to disseminate narratives favourable to its interests, technical research and investigative journalism can contribute to countering these activities. Policy responses need to correspond to the security and human rights implications of these operations and limit the capacity of the perpetrators.

4) Measuring the impact of Iran's information influence operations is a complex question that calls for enhanced research support and resources. Establishing a baseline of the effect of these narratives requires sustained data collection and contact with the target populations to bolster longitudinal and comparative research. Thus far, limited research has been done on this front. This could change with grants and extended security arrangements for researchers in the field.

5) Counter-responses to Iran's narratives need to be multi-faceted and mitigate the disparity of resources between civil society and Iran's disinformation apparatus. Counter-responses must transcend the information domain and address the long-term political, economic, and human aspects of life in conflict-affected societies like Syria. Achieving these objectives requires the EU to support actors with local knowledge of the nuanced circumstances and to commit to post-war

[103] DFRLab, op. cit.
[104] As an interviewee who wished to remain anonymous for security reasons pointed out. The interview was conducted during the course of this study on August 26, 2021.

development in the form of aid and transfer of skills and resources that remain scarce on the ground.

3.2 The People's Republic of China's interventions in Taiwan

One of the key strategic objectives of the PRC is reunification with Taiwan[105]. The incumbent government of Taiwan (led by the DPP), civic activists, and concerned domestic and foreign observers have adopted a vigilant attitude towards any influence activities undertaken by the PRC. They therefore commit a great deal of resources to revealing and countering the use of social media and other communication channels by (pro-)PRC actors that aim to nudge public debates and political trends on the island so that they better align with Beijing's strategic goals.

3.2.1 State of play

A frequently cited Varieties of Democracy (V-Dem) study by the reputable project based at the University of Gothenburg[106] considers Taiwan to be a democracy that is most vulnerable to external disinformation. Top security institutions on the island share this concern. In May 2019, the National Security Bureau published a report titled 'Countermeasures Against Chinese Disinformation Psychological Warfare', and delivered it to the Legislative Yuan, Taiwan's parliament[107]. The report argued that China is taking advantage of Taiwan's openness. It also suggested that China is spreading 'disputed information' and engaging in psychological and cognitive warfare, with a goal to divide, distract, and weaken Taiwan's security capacities[108]. PRC entities and/or agents are believed to be leveraging their improved financial position[109], which enables them to pay 'for coverage in various publications and on a television channel'[110]. However, 'information operations' in the digital domain, and in particular on social media, have much further-reaching consequences than those in traditional media, such as TV. Historically, digital domain campaigns have been associated with the internationalisation of paid commentators[111], as well as isolated bots and trolls on social media that primarily post reactive comments online. By 2018, the repertoire of Chinese actors' digital activities had greatly expanded. In the wake of the 2019 Hong Kong protests, which became a central issue in Taiwan, researchers identified a large network of inauthentic accounts on social media networks based in Mainland China. These accounts had long periods of dormancy and bursts of active posting of original content, some of which was taken down by Facebook, Twitter, and YouTube on the grounds of being connected to PRC state institutions[112]. Researchers cannot conclude whether this network has been run by a single organisation, or is a product of different endeavours ran by different organisations[113]. Activists from Taiwan point out that the seemingly decentralised way of conducting online activities is what distinguishes Chinese from Russian activities in the digital domain (the latter being more centralised).[114] An in-depth analysis of the banned accounts revealed 'active and prolific, but ultimately low-impact, cross-platform political spam network in Chinese', and a 'far less professional' amplification network, whose contents, according to Graphika, was produced with limited resources[115].

[105] This goal has been reiterated by the Chinese President Xi Jinping during the celebration of the centenary of the founding of the Communist Party of China in 2021. See Sacks, D, 2021, 'What Xi Jinping's Major Speech Means For Taiwan', Council on Foreign Relations.
[106] Walsh, E., Disinformation in Taiwan: International Versus Domestic Perpetrators, V-dem, 2020.
[107] National Security Bureau, Countermeasures Against Chinese Disinformation Psychological Warfare [中國假訊息心戰之因應對策], May, 2019.
[108] See Bayer, J. et al., op. cit., 2021.
[109] Huang, J., The China Factor in Taiwan's Media, China Perspectives [Online], 2017/3.
[110] Lee, Y., Cheng, I., Paid 'news': China using Taiwan media to win hearts and minds on island – sources, Reuters, 2019.
[111] Yang, G., 'Internet Activism & the Party-State in China', *Dædalus* 143 (2), 2014.
[112] Lee, D., Hong Kong protests: Twitter and Facebook remove Chinese accounts - BBC News, 20 August, 2019.
[113] Nimmo, B., et al, Return of the spamouflage dragon, Graphika, April, 2020.
[114] Interview with Ttcat, 1 September 2021.
[115] Nimmo, B, et al., Cross-Platform Spam Network Targeted Hong Kong Protests, Graphika, September, 2019

The shutting down of thousands of accounts by the social network's administrators, however, did not break this network, which endured, and has grown over time, although with limited success when it comes to impacting democratic deliberation[116].

With the increase in activity of Chinese diplomats on Twitter (a process that often is described as the rise of a 'wolf warrior diplomacy')[117], there is often interaction between social media accounts perceived as suspicious by researchers and those of Chinese officials (i.e. they would retweet each other). According to Graphika, nevertheless, Chinese diplomats do not necessarily engage in spreading disinformation with prior knowledge or intention[118]. Social media influencers with large followings from all over the world sometimes also engage with the suspicious accounts and share the accounts' content, including disinformation and misinformation[119]. These accounts sometimes echo official PRC narratives and express support for China (and opposition to the US), which does not automatically qualify them as spreading disinformation; however, there have also been instances where the content that they shared was determined to be disinformation by reputable fact-checkers. The fact that the suspicious accounts have been anonymous has made it difficult to seek liability and accountability. Nevertheless, despite their growing following and reach, Graphika notes that the successes of these networks 'are still sporadic'[120]. Only a 'handful' of the hundreds of accounts identified have managed to 'break out' of the echo chamber, though it is to be expected that they will become more sophisticated in the future[121].

Disinformation on Taiwan's social media gained particular intensity during the 2018 local elections and referenda, as well as during the 2020 general election. In 2018, a number of contentious narratives mushroomed, including (but not limited to) accusations made against political candidates by anonymous overseas accounts, claims about China assisting Taiwanese travelers caught in a typhoon in Japan who identify as Chinese, and scripted testimonies about the socio-political realities on the island presented as actual news.[122] As a result of the disinformation noise prior to the election, on election day about 50 % of voters casting their ballot did not have a clear idea which narratives pertinent to the local elections and referenda were true and which were false[123].

Policymakers and researchers saw this as an outcome of Chinese information operations. A DoubleThink Lab report posited that by 2020, the 'Chinese government no longer trie[d] to conceal these operations', conducting them 'boldly and explicitly'[124]. The report argues that while President Tsai (the candidate disliked by Beijing) was smoothly re-elected, and while individual pieces of content originating from or being linked to various PRC actors (military, government, business or individuals) may not have had significant impact in isolation of one another, their cumulative long-term effect should not be underestimated[125]. The report distinguishes between four different forms of 'information operations' that they link to the PRC – propaganda (i.e. content originating from the government), 'pink mode' (spontaneous mobilisations of CCP supporters), content farms (i.e. mass content production outsourced to content farms), and collaboration (content production 'funded by China, made in Taiwan'). The latter two

[116] Nimmo, B., et al., op. cit., 2020.
[117] Brandt, J., Schafer, B., How China's 'wolf warrior' diplomats use and abuse Twitter, Brookings, 2020
[118] Nimmo, B. et al, Spamouflage Breakout, Graphika, February, 2021
[119] Ibid.
[120] Ibid.
[121] Ibid.
[122] Wang, T., 'Does Fake News Matter to Election Outcomes?: The Case Study of Taiwan's 2018 Local Elections, *Asian Journal for Public Opinion Research*, 8(2), 2021, pp. 67–104. DOI:10.15206/ajpor.2020.8.2.67.
[123] Ibid.
[124] Lee, L. et al., Deafening Whispers China's Information Operation and Taiwan's 2020 Election, DoubleThink Lab, 2021.
[125] Ibid.

are considered to have been much more effective than the former[126]. While the actual message of the content diffused through content farms and collaboration has not been directly pro-PRC[127], the most significant narrative echoed during the 2020 elections was that 'democracy is a failure' – a message aiming to sow distrust in the political system of Taiwan[128].

The COVID-19 pandemic started as Taiwan was heading for the voting booths. Social media in Taiwan has seen no shortage of spectacular rumours and 'paranoid' internal debates related to COVID-19, the public health care system, vaccines, etc.[129] The central contentious issues in the COVID-19 debate were: the nature of the disease; the logic of the contagion; preventive measures and remedies; potential cover-ups by Taiwan; and the relative incapacity of Western governments to match China's model of coping with the disease[130]. In the early stages of COVID-19, a large number of social media accounts copy-pasted and re-shared the same disinformation content[131].

The attribution of disinformation on Taiwanese social media to the PRC needs important caveats. Activists point out that even when content can be traced to Mainland China, it takes much more elaborate analysis to demonstrate a convincing link with CCP or the PRC institutions[132]. As pointed out by the IRI/Graphika and the Stanford Internet Observatory reports, there is still a shortage of convincing evidence linking PRC state institutions with particular episodes of heightened disinformation in Taiwan[133]. Furthermore, Taiwanese rather than Mainland actors are becoming more active in spreading both misinformation and disinformation, as well as emotional, biased, and heavily opinionated content on Taiwan's social media[134]. Due to the linguistic differences, such content 'appears to be produced in Taiwan'[135]. Agents who produce or disseminate it are not necessarily directly co-opted by PRC. They could potentially be associated with influential actors from Taiwan with commercial or other interests in the Mainland[136]. Social media activities may also have simply been outsourced to them[137].

With the rise of the content creator economy funded through donations, there has also been a rise in the 'disinformation market'. Some of the leading Taiwanese YouTubers, in order to attract donations, are considered to be disseminating disinformation, misinformation, and emotional, biased, and heavily opinionated content, while also raising funds directly from the PRC (e.g. they use Chinese digital finance services, such as Alipay or WeChat Pay)[138]. The targets of Chinese-language content on social media suspected to be linked to the PRC in some shape or form are not only people in the region, but also the growing Chinese diaspora, especially those who are keener on using Western rather than PRC-based social

[126] The activist website IORG also claims that 'local collaborators' are critical in spreading Chinese information manipulation in Taiwan. See Defending Democracy Against Authoritarian Expansion, IORG, 2021.
[127] Interview with Puma Shen, 14 September 2021.
[128] Other narratives included: 'Green Terror' (repressive rule of the DPP), Tsai Ing-Wen is incompetent, DPP is a client to the US, US is plotting against China, Taiwan's prosperity depends on good relations with Beijing, etc. Ibid, p. 44.
[129] Hioe, B., Between Infodemic and Pandemic: The Paranoid Style in Taiwanese Politics, Popula, 22 July, 2021.
[130] Tseng, P. and Shen, P., The Chinese infodemic in Taiwan, DoubleThink Lab, 2020.
[131] Interview with Ttcat of the DoubleThink Lab, 1 September 2021.
[132] Interview with Puma Shen of the DoubleThink Lab, 14 September 2021.
[133] In lieu of strong evidence, claims that certain accounts on social media originating from China being linked to the Chinese state are often based on inference, e.g. the production of a large volume of original videos (which means that someone resourceful had to produce them), the timing of the activity of these accounts (which strongly correlates with working hours in PRC and dips during Chinese public holidays) and the fact that to be active on social networks that are banned in the PRC, Chinese users need a VPN, which is increasingly sanctioned when used by Chinese netizens (but not by government employees). See Cook, S., Beijing Is Getting Better at Disinformation on Global Social Media – The Diplomat, 30 March, 2021.
[134] Lee, L. et al., op.cit., 2021.
[135] Committee to Protect Journalists, 2019, One Country, One Censor: How China undermines media freedom in Hong Kong and Taiwan.
[136] Ibid.
[137] Lee, L. et al., op.cit., 2021.
[138] Interviews with Ttcat and Puma Shen of the DoubleThink Lab.

media[139]. Finally, one of the often-overlooked goals of the activities on social media initiated by the PRC is simply creating an inflated image of China's impact on others, which then serves the primary purpose of appearing particularly strong in front of a domestic (PRC) nationalist audience, meaning that the effects abroad are of secondary importance[140].

Furthermore, the importance of the PRC impact notwithstanding, in the run up to the 2020 general election, it became evident that internal divisions are a significant challenge for Taiwan's democracy. As the Stanford Internet Observatory reports, 'we did not find any cases of disinformation on social media that we believed to be attributable to the PRC' but 'did note some suspicious activity [tied to] domestic hyper-partisan fan groups'[141]. This is, in the first place, a result of the political polarisation between the DPP and the Nationalist Party, Kuomingtang (KMT), and the respective swaths of society that stand behind them[142]. In the month leading up to the 2020 elections, Facebook had shut down '118 fan pages, 99 groups, and 51 accounts' supportive of presidential candidate Han Kuo-yu of KMT for violating its guidelines[143]. Beyond the DPP-KMT split, polarisation and disinformation have been linked to the new divisions within Taiwan's progressive camp itself[144]. The extremely polarised and warfare-like political culture on the island is a significant obstacle in the struggle against disinformation; often, one can see members of the opposition blaming the DPP government for weaponising the combat against external disinformation to crack down on political opponents[145]. Geopolitical trends (such as the aftermath of the withdrawal of American troops from Afghanistan and the potential consequences for Taiwan) have recently become a major subject of politicisation[146].

Finally, political content occupies a significant share in the pool of disinformation, but another type of content is ever more prevalent, even prior to the COVID-19 pandemic: the most widespread harmful content concerned public health[147]. Health-related disinformation follows recurrent patterns and schedules. For example, whenever same-sex marriage becomes an issue, AIDS-related disinformation and misinformation spreads on social media[148], while during the persimmon (a type of fruit) season, food-related disinformation and misinformation does[149]. Online shopping has also fallen prey to scams and other dubious content[150], showing that not only macro-level political developments, but also all sorts of daily activities can be disrupted by disinformation.

COVID vaccinations have been also a subject of disinformation. In this case, different political and commercial interests have intersected: the distributor for the publicly preferred Pfizer vaccine has been the Shanghai-based Fosun Pharma, and the key actor for procuring the vaccine to Taiwan has been the billionaire Terry Gou, founder of Foxconn, who has significant business interests in the PRC[151].

In sum, the endeavours by PRC and Taiwan's domestic political culture together present the government and activists with a particular challenge when it comes to preserving the integrity of public deliberation. Potentially harmful content promoted from abroad finds fertile ground in Taiwan. This presents the

[139] Influencing overseas Chinese by tweets: text-images as the key tactic of Chinese propaganda | SpringerLink
[140] Monaco, N. et al., Detecting Digital Fingerprints: Tracing Chinese Disinformation in Taiwan, IRI&Graphika, August, 2020.
[141] Stanford Internet Observatory, Taiwan Election: Disinformation as a Partisan Issue, 2020.
[142] Aspinwall, N., Taiwan's War on Fake News Is Hitting the Wrong Targets, Foreign Policy, 10 January, 2020.
[143] Strong, M., Facebook shuts down groups supporting Taiwan KMT presidential candidate, Taiwan News, 2019.
[144] For instance, the pro-independence 'Formosa Alliance' that had split from the DPP was identified to be behind the spread of the rumours that President Tsai had a fake PhD degree. Aspinwall, N., Taiwan President Sues Scholars for Alleging Her Doctorate Degree is Fake, The Diplomat, 7 September, 2019.
[145] Interview with Cofacts, 14 September 2021.
[146] Interview with Ttcat, 1 September 2021.
[147] Cofacts Interview Notes [TheDiplomat], 10.2018
[148] 20180516 - RightsCon 2018 - cofacts - Google Slides
[149] 20180516 - RightsCon 2018 - cofacts - Google Slides
[150] Cofacts Interview Notes [Taipei Times], 06.2018
[151] Interview with Ttcat, 01.09.2021.; also see Foxconn's Gou hopes for up to 9 mln BioNTech shots for Taiwan this year, Reuters, 07 September 2021

authorities and civil society actors with a particular challenge in disentangling the different sources of harmful content, and its various manifestations.

3.2.2 Targeted groups in Taiwan

Victims of disinformation, misinformation and mal-information fall into different categories.

On the one hand, there are the people who are portrayed by the information and who may see their public perception changed, often negatively, by false or misleading information. This is particularly true of, for example, LGBTQ+ persons, who have been targeted by homophobic and transphobic rhetoric. This was the case around the time of the referendum on same sex marriage in 2018, and has also been the case whenever the question resurfaces. For these victims, fact-checking alone may not suffice to correct the narrative, as disinformation and misinformation interact with deep-seated prejudice and intolerance.

A second category of people who may be considered victims are the people who are taken in by false or misleading information. People of all ages may believe disinformation and misinformation, although activists and policymakers in Taiwan have tailored their response to different ages. Taiwan has tried to increase media literacy for the different age groups, to create technological solutions for those with lower media literacy, and to stimulate inter-generational solidarity and assistance in the process of fact-checking.

Among consumers of disinformation, the safety or health of some people have been directly affected by disinformation or misinformation. These include people who survived natural or other disasters, and who were targeted in sensational news in the aftermath of these disasters; or people with particular health problems, targeted by the great quantity of health-related misinformation and disinformation. The potential dangers of this were one of the reasons that Taiwan's government developed a rapid response system.

3.2.3 Taiwan's response

As a relatively new democracy, Taiwan has a particular history of combating disinformation. Spreading political rumours has been legally sanctioned since 1991 as a crime that is punishable by up to three days in jail and a fine of up to 30,000 NTD[152]. In 1999, the Taiwan Media Watch was established, a non-profit collaboration of academic, media, and civil society figures who monitor and evaluate media content with the goal of 'maintaining press freedom, carrying out media justice, promoting media self-regulation, and protecting the public's right to know'[153]. The government has pushed for introducing media literacy as part of regular education curricula since 2002[154]. Disinformation has also been sanctioned under the Civil Servants Election and Recall Act and the Presidential and Vice-Presidential Election and Recall Act[155]. As the experience with SARS in 2003 was an important lesson showing that disinformation spreads alongside infectious disease, disinformation regarding epidemics has been sanctioned under the Communicable Disease Control Act[156]. Similarly, natural disaster-related disinformation is sanctioned with the Disaster Prevention Act[157]. Disinformation related to product quality and price manipulation has been sanctioned under the Criminal Code[158].

The legal and policy framework was further upgraded after President Tsai of DPP entered power in 2016. The Legislative Yuan passed a long-debated and contested Anti-Infiltration Act (AIA) on 31 December

[152] Social Order Maintenance Act, Laws & Regulations Database, 2021.
[153] Taiwan Media Watch, official website.
[154] Media Literacy Education Resource Network (媒體素養教育資源網), official website of the Ministry of Education of Taiwan.
[155] Bayer, J. et al, op. cit.
[156] Ibid.
[157] Ibid.
[158] Ibid.

2019[159]. In 2019, media literacy was finally introduced into the national education curriculum, which focused on preparing students to properly filter and double-check online content[160]. After the appearance of COVID-19 in the PRC, Taiwan also enacted the Special Act for Prevention, Relief, and Revitalisation Measures for Severe Pneumonia with Novel Pathogens, which also addresses the spread of disinformation (i.e. making it punishable by up to three years of prison and up to NTD 3 million in fines).

AIA is of particular importance here. It was adopted on the eve of the presidential elections in 2020, in tense circumstances, amid controversy arising from the claim by an ousted Chinese spy that three important media outlets in Taiwan (CitiTV, China Television, and Eastern Broadcasting Co) worked for the PRC[161]. AIA sanctions political activities that are directed, financed, or coordinated by a foreign power, which include political campaigns and canvassing, lobbying, donating to a party, interfering in rallies or public assemblies, disturbing the public order, and spreading election-related disinformation. Engaging in such activities is punishable by imprisonment of up to five years and fines of up to NTD 10 million. However, AIA does not address the flow of information itself, as the government advocates preserving freedom of expression even amidst cracking down on foreign disinformation. In that sense, AIA deals primarily with identifying and penalising the source of disinformation, if the source works for a foreign government[162]. AIA has been contested by the opposition, who saw it as an anti-democratic measure, whereas global watchdogs such as CPJ noted potential negative effect on the freedom of expression and the press, as well as instrumentalisation of the disinformation struggle[163]. On the opposite side of the spectrum, AIA has been criticised by civic activists concerned about the PRC's interference in the island's affairs for the act's perceived insufficiencies; these activists have argued for a US-style Foreign Agents Registration Act and for complete transparency on ownership and sponsorship ties[164].

Under the DPP, the enforcement of existing regulation on traditional media has been stricter than before. The best-known example is the motion of the National Communications Commission (NCC) to reject the broadcasting license renewal application made by Chung Tien Television (CTiTV) for its channel CTi News, which has since ceased to operate[165]. CTi News was the subject of hundreds of complaints for its biased reporting. The TV station was owned by Tsai Eng-meng, an entrepreneur (owner of WantWant Holdings Ltd) with substantial commercial interests in PRC. The opposition expressed grave disagreement with and disappointment in what they saw as a threat to press freedom. Reporters Without Borders expressed regret over the decision of the NCC, but said it did not go against press freedom[166].

The struggle with disinformation presents Taiwan with the challenge of maintaining freedom of expression. Opposition representatives have consistently complained that the legislation infringes on free speech[167]. Moreover, as Taiwan is often taken as an example by other actors in East and Southeast Asia, the development of strict legislation is seen as potentially having net negative effect for democracy in the region. Brian Hioe, a well-know journalist and activist, has contrasted the restrictive measures pushed by progressives in Taiwan as a response to rising disinformation, arguing that similar restrictive endeavours have been or could be undertaken by autocratically leaning governments throughout Asia with the goal

[159] Legislative Yuan Passes Anti-Infiltration Bill to Strengthen Defense for Democracy and Preserve Stable and Orderly Cross-Strait Exchanges, Mainland Affairs Council, 31 December 2019.
[160] Media Literacy Education Resource Network (媒體素養教育資源網), official website of the Ministry of Education of Taiwan.
[161] Yang, S., Executives of 3 Taiwan TV stations named by 'Chinese spy' invited to NCC meetings, Taiwan News, 26 November 2019
[162] Bayer, J., op.cit., 2021.
[163] Committee to Project Journalists, 2019, op. cit.
[164] Interview with Puma Shen 14 September 2021.
[165] Taiwan Shuts Down Pro-China CTi News, The News Lens, 19 November 2020
[166] Taiwan: the non-renewal of CTi news channel's licence does not go against press freedom, Reporters Without Borders, 20 November 2020.
[167] Chou, B., Taiwan's Proposed Bills To Regulate Online Content Stir Outrage, The News Lens, 17 December 2020.

of suppressing dissent[168]. Finally, as a CPJ report posits, legislative measures alone 'don't seem well designed to cope with [...] a possible deluge of coordinated social media surreptitiously posted by China or its surrogates'[169].

The limitations of a regulation-based approach have thus prompted Taiwan to seek different solutions and upgrade its anti-disinformation drive. The person who contemplated and implemented a number of innovations in this regard was Digital Minister Audrey Tang, a software engineer[170]. Minister Tang devised a proactive and inclusive (whole-of-society) approach, based on pre-emption and early and rapid response to disinformation. Some of the steps it includes are a) collaboration with global social media companies to tackle viral disinformation content on their platforms; b) support of independent local fact-checking services; and c) moving from reaction to pro-action, i.e. through stimulation of new debates via online platforms and finding new ways to ensure active civic participation.

In practice, Tang's method consists of constant tracing of social media trends, identifying potential hotpots of disinformation, and promptly deploying an effective and viral counter-campaign that conveys what the government and fact-checkers have assessed as truthful information. The goal is not only to reach out to individuals on social media, but rather to pre-empt the hijacking of the news cycle, i.e. to offer a counter-narrative to the traditional media outlets, which can often amplify untruthful messages in the hunt for sensational news that is more clickable[171]. This model of responding to disinformation, instead of relying on legal control, is based on collaboration with social media platforms to ensure 'co-governance'. In addition to the tech front, the model also foresees 'increasing oversight and transparency on political advertisement, and strengthening media competency across all age groups', as well as cooperating with third parties in order to 'build an independent, transparent, and fair supervision mechanism'[172]. Given its resourcefulness, it is imperative for the government 'to provide timely, accurate, and easy-to-understand information to the public and to allow third parties to fact-check'[173]. One of the guiding principles is 2-2-2: a response of 200 characters or less should follow within 20 minutes of the identification of disinformation content, and 2 images should accompany this response (to make it more appealing). In the process, humour is weaponised ('humour over rumour')[174]. This approach was further advanced during the COVID-19 pandemic, where – under the principle of 'Fast, Fair, and Fun' – Taiwan leveraged technological solutions to overcome the problem of distributing masks (fast reaction, fair distribution, often with humorous tint)[175].

Complementing this elaborate anti-disinformation strategy, Taiwan also aimed to improve public trust. One way to do so was to leverage technology to maximise the transparency of the system (i.e. by streaming various meetings and forums publicly and allowing interaction with the audience). During the COVID-19 pandemic, regular public conferences were held, with the goal of streamlining the official messaging and making sure it had been received[176]. Citizens were invited to actively take part in public deliberations through innovative software tools[177].

[168] Committee to Protect Journalists, 2019, op. cit.
[169] Committee to Protect Journalists, op. cit., 2019.
[170] Kerr, W., Phillips, M., Taiwan Is Beating Political Disinformation. The West Can Too., Foreign Policy, 11 November 2020.
[171] Committee to Protect Journalists, 2019, op. cit.
[172] A conversation with Audrey Tang, Fondation pour la Recherche Strategique, April, 2020.
[173] Ibid.
[174] Ibid.
[175] Hsieh, M., Fast, Fair, Fun: Taiwan Digital Minister Audrey Tang On Pandemic Response, Ketagalan Media, 6 February, 2021.
[176] Daniels, R., Taiwan's unlikely path to public trust provides lessons for the US, Brookings Institution, 15 September, 2020.
[177] Nabben, K., Hacking the pandemic: how Taiwan's digital democracy holds COVID-19 at bay, The Conversation, 11 September, 2020.

Aside from the agile approach devised by the government, Taiwan has also seen a wide and genuine mobilisation of civil society activists, and 'civic tech' engineers and scholars in the struggle against disinformation. They have been led by the ideal of achieving '(online) deliberation without inauthentic information'[178]. Aware that disinformation cannot be fully eradicated, they work on empowering civic resilience and counter-strategies[179]. Some of the key actors include Cofacts, a civic tech initiative which provides assessment of various news items in real time and has developed a chat-bot integrated with instant messenger LINE, and the FactCheck Center, which maintains a database of all sorts of disproven claims. A more thorough analysis of disinformation and the role of PRC has been provided by the DoubleThink Lab. While these activists have collaborated with the government, they have attempted to stay independent and avoid getting entangled in political confrontation[180]. Some of them have been critical of the approach of the government, arguing that it is overly focused on debunking 'fake news', and that the approach, despite its successes, has at least two fault lines: 1) it overlooks the 'big picture' in terms of the origin and long-term challenge posed by disinformation; and 2) it is condescending towards those who, due to the lack of thorough understanding, have believed or further spread disinformation, leaving little room for dialogue[181]. Activists also problematise the very logic of the true-false dichotomy that inevitably emerges during anti-disinformation campaigns as having limited efficacy; they instead propose a strategy of diversification of views and dialogue[182]. They argue that the government approach does not sufficiently distinguish between harmful and benign disinformation, and between production and dissemination, often investigating and pressuring gullible individuals for spreading relatively harmless content that they have not created themselves, but stumbled upon online[183].

3.2.4 Conclusions and lessons learnt

In terms of understanding the vulnerability to malicious activities on social media, and in particular, the potential role of external actors, Taiwan offers an important lesson that the external and the internal dynamics of spreading disinformation, misinformation, and emotional, biased, and heavily opinionated content, as well as conspiracy theories, are deeply intertwined. The impact of PRC notwithstanding, internal divisions and polarisation in Taiwan itself make the island's democracy particularly vulnerable. Polarisation is on the rise in a number of democracies around the world, and social media often facilitate this process, including in the EU[184].

The government of Taiwan nominally promotes an approach of dealing with misinformation and disinformation that does not rely on censorship or sanctioning, but rather on a proactive, engaging strategy and mobilisation of social media companies and civil society actors[185]. While changes in the domestic legislation do raise concerns about the freedom of expression, the government has performed better with regards to the proactive component of its strategy. The pre-emptive, creative and, above all, rapid approach to debunking misinformation and disinformation on social media aims to prevent harmful social media content becoming viral and reaching traditional media. The 'meme engineering' method foresees adaptation and instrumentalisation of the new internet language and culture, with the goal of making the message viral. Teams of meme engineers have been installed in various governmental

[178] Interview with Ttcat of the DoubleThink Lab, 1 September 2021.
[179] Interview with Ttcat of the DoubleThink Lab, 1 September 2021.
[180] Interview with Puma Shen of the DoubleThink Lab, 14 September 2021.
[181] Interviews with Ttcat (1 September 2021) and Puma Shen (14 September 2021) of the DoubleThink Lab.
[182] Interview with Cofacts, 14 September 2021.
[183] Interview with Cofacts, 14 September 2021.
[184] Dixon, T., Juan-Torres, M., Is the Internet Eroding Europe's Middle Ground?, European Strategy and Policy Analysis System, March, 2018
[185] Interview Taipei Times 2018.6 [EN] Taipei Times - Google Docs

departments or agencies to carry out these tasks. Such an understanding and instrumentalisation of memes is significantly different from the EU's approach[186].

Beyond the government, civil society has played a central role in the process. Given that disinformation may only intensify in the future, the most feasible approach to handling the predicament of spreading such content on social media is a combination of technology-oriented solutions with human creative power. Technological solutions are the baseline; for example, automation of responses through a chatbot (such as the one created by Cofacts) significantly helps in raising the responsiveness level, although the sustained positive outcome still depends on hard and cumbersome human input[187]. Solutions such as the Cofacts chatbot are intended to assist those who are not proficient in fact-checking, but are keen on forwarding items via instant messaging (in the case of Taiwan, disinformation spreads via shared messages in chats or closed groups on LINE, a leading messenger app in Asia, with a 90 %+ adoption rate in Taiwan)[188]. Such solutions are not focused on producing detailed reports debunking information (i.e. traditional fact-checking), but rather provide an accessible channel that provides a quick assessment of the questionable items and links to detailed reports provided by fact-checkers[189]. Allowing readers to upvote or downvote evaluations on their website serves as a form of quality assurance[190]. Other quality assurance strategies could be found in the experience of collaborative knowledge-production websites, such as Wikipedia, Quora, or StackOverflow.[191] Such a model, however, depends on volunteers' commitment, which varies over time and sometimes leads to a shortage of editors[192] as well as 'deep fatigue'[193].

Transnational cooperation is of particular importance. COVID-19, for example, overwhelmed fact checkers, both in terms of the increase of content submitted for evaluation, but also in terms of the novelty of the challenge; one way to overcome this was collaborating within and across borders[194]. The DoubleThink Lab activists see the problem of disinformation and the role of the PRC as a major global challenge, and are now working on generalising and globalising their insights and applying them at a global scale[195].

Improving media literacy, awareness, and vigilance is a core objective in any strategy dealing with disinformation. While malicious intentions and a particular disruptive agenda may be behind the creation of disinformation content, disinformation would not matter if it were not believed and shared. One way that Taiwanese authorities and civic tech activists have worked to stop the spread of disinformation is by adopting an age-sensitive approach[196]. In fact, people of different ages have been shown to judge the veracity of information differently[197], and Taiwan's efforts have included cross-generational programmes, including by encouraging younger internet users help their family members by sending them an evaluation of various items of news content shared online. Taiwan has also worked generally to improve media literacy[198].

[186] Tu, C., Lessons from Taiwan's experience with COVID-19, Atlantic Council, 7 April, 2020.
[187] Cofacts Interview Notes [Taipei Times], June, 2018.
[188] Cofacts Interview Notes [ITS Rio], October, 2019.
[189] Cofacts Interview Notes [DW Brazil], July, 2018.
[190] Cofacts Interview Notes [ITS Rio], October, 2019.
[191] Cofacts Interview Notes [Splice], July, 2018.
[192] Chang, H. et al., 'Digital Civic Participation and Misinformation during the 2020 Taiwanese Presidential Election', *Cogitatio* 9/1.
[193] Interview with Cofacts, 14 September 2021.
[194] Cofacts Interview Notes [L'Usine Digitale], March, 2020.
[195] Interview with Puma Shen, 14 September 2021.
[196] Cofacts Interview Notes [ITS Rio] September 2018 and October 2019.
[197] See, e.g. Brashier, N.M., Shacter, D.L., Aging in an Era of Fake News, Current Directions in Psychological Science, 2020, Vol. 29(3), 316–323; Vijaykumar, S., et al., How shades of truth and age affect responses to COVID-19 (Mis)information: randomized survey experiment among WhatsApp users in UK and Brazil, Humanities and Social Science Communication 8, 88 (2021).
[198] Yang, O., Defending Democracy Through Media Literacy, Taiwan Democracy Bulletin, 2019, Vol. 3, No. 6.

A related challenge involves social bonds and trust. The case of Taiwan shows that users may be inclined to trust certain sources or individuals (close or not) more than their own judgment[199]. In this sense, combating disinformation by a head-on confrontation may sometimes end up straining even inter-personal relations.

Any endeavour that deals with disinformation has to mind the thin line between outright falsehoods and different opinions and biases. To avoid incorrect or unfair labelling of different opinions as disinformation, for example, Cofacts tries to discern between opinionated content, as opposed to content spreading disinformation and misinformation, and encourages discussion and inclusion of different opinions for any news item that it addresses[200]. DoubleThink Lab activists also note that there are nuances between outright inaccurate facts and interpretations and conspiracy theories[201]. A structural challenge on the other hand, is the ubiquity of suspicious content – not only does it never stop, but its volume increases over time[202]. Some disinformation activities exploit marketing tricks and are based on promises of discounts, free products, free access to services, etc. These are scams that take advantage of gullible customers[203]. This also reveals another paradox which helps in the dissemination of disinformation: disinformation is always free and frequently reproduced, while legitimate news items are often copyrighted, strongly protected, and hidden behind paywalls, as well as generally much less accessible to mass audience.

Finally, the input side of the process has been often neglected in the studies on disinformation and misinformation in Taiwan. For instance, Beauchamp-Mustafaga and Drun argue that the majority of the existing literature (that this report also relies upon) focuses primarily on the potential outputs (i.e. what we actually see on social media) and effects of the PRC's attempts to impact social media debates in Taiwan, and on potential countermeasures; such an approach, they posit, does not grasp the long-term strategy behind the use of social media to advance the PRC's agenda[204]. One way to remedy this, according to these scholars, is to focus less on the outputs and on the countermeasures enacted by Taiwan, and to look more deeply into the relatively easily available documents and debates coming from the PRC, which reveal the 'stated intentions and tactical considerations' of the PLA (People's Liberation Army) and the Chinese government.[205] In their own contribution, these authors explore the role of the Taiwan-focused PLA Strategic Support Force Base 311, concluding that it 'may have executed a campaign to covertly manipulate Taiwanese social media and interfere in Taiwan's 2018 elections'[206]. Their approach also emphasises the 'near-impossibility in definitively attributing disinformation to a concrete origin', as well as the 'well-documented difficulties in attribution of inputs'[207]. The lesson to be drawn here is that suspicious social media activities and disinformation in general could be better understood if studied as part of a larger endeavour that significantly focuses on the input side of the process. The DoubleThink Lab in Taipei now works on tracing the inputs based on writing style – as they point out, different actors in China have different styles and messaging, and different strategies[208]. On the other hand, the approach by Cofacts is different – they argue that pinpointing the source of dubious content would do little to dispel belief in and support for the narrative such content promotes[209].

[199] Cofacts Interview Notes [TNLi], September, 2018.
[200] Cofacts Interview Notes [DW Brazil], July, 2018.
[201] Interview with Puma Shen, 14 September 2021.
[202] Interview with Cofacts, 14 September 2021.
[203] Cofacts Interview Notes [TNLi], September, 2018.
[204] Beauchamp-Mustafaga, N., Drun J., Exploring Chinese Military Thinking on Social Media Manipulation Against Taiwan, China Brief, April, 2021.
[205] Ibid.
[206] Ibid.
[207] Ibid.
[208] Interview with Puma Shen, 14 September 2021.
[209] Interview with Cofacts, 14 September 2021.

In light of the analysis, the following specific lessons can be learnt:

1) While the focus of policymakers and experts has been on the role of foreign interference and influence, the example of Taiwan shows that the local context and local agents are major enablers and facilitators. In terms of the context, the divisions and polarisations in Taiwan's society provides fertile ground for disinformation and misinformation to spread. In addition to particular political agendas, local actors may spread disinformation because of their commercial interests, given the economic interdependence between the PRC and Taiwan .

2) The case of Taiwan also shows the limit of the conventional understanding of harmful content and the logic behind its diffusion. Taiwanese activists and fact-checkers have been particularly challenged by the diffusion not necessarily of falsehoods or misleading content, but also of emotional, biased, and heavily opinionated and polarising content. Polarisation stifles online deliberation and helps fuel disinformation and misinformation. Addressing the problem of the cumulative and intertwined effects of these two different sets of challenges is central to the preservation of democratic culture. This requires better conceptualisation (i.e. by proposing an alternative to established concepts such as disinformation and misinformation), and avoiding the trap of establishing truth-setting authorities. The initial solutions provided by Taiwanese fact-checkers is case-by-case analysis, and distinguishing between actual falsehoods and heavy opinions. However, the interplay between disinformation, bias and polarisation remains a crucial problem in the case of Taiwan.

3) While Taiwan's legislative amendments are of questionable value for democracies worldwide, its proactive, whole-of-society approach focused on pre-empting and neutralising misinformation and disinformation, and other types of content of questionable legitimacy, offers important lessons. The government has created a favourable environment for civic tech engineers, fact-checkers, and other volunteers to proactively deal with harmful content. The key step in this direction has been the hiring of civic tech activist Audrey Tang as Digital Minister.

4) Media literacy (or rather lack thereof) and its enabling role in the spread of disinformation and misinformation has been a major challenge for Taiwan. To tackle this, the government has invested in developing media literacy programs. However, a key role has been played by civic tech and other activists who promoted a culture of inter-generational solidarity and friendly 'review' of content shared.

5) Cooperation with social media corporations is crucial for reining in disinformation and misinformation. Such cooperation does not only have a direct effect on the problem, but it also helps involve others in coming up with solutions. In the case of Taiwan, cooperation between the authorities and LINE has empowered civic tech engineers to offer innovative solutions (i.e. integrate fact-checking tools in the app).

6) While memes are often associated with harmful content, the case of Taiwan shows that they can be 'weaponised' to counter disinformation and misinformation. The production of easily digestible and viral content by the government, as well as activists, has helped in dispelling falsehoods.

7) The experience of Taiwan shows that while there is a trend of moving reliable news behind paywalls, where it is not as easily accessible, 'fake news' is free and increasingly abundant. In other words, more and more people have to search for legitimate information, while misinformation and disinformation reaches them easily. To a great extent, the work of fact-checkers and activists in Taiwan has been focused on bringing legitimate information to the audience. Making legitimate information more broadly available and easily accessible should be a priority for any institution combating disinformation and misinformation.

8) Misinformation and disinformation often spread through inter-personal communication. There are limits to any endeavours to confront them heads-on. In the case of Taiwan, fact-checkers and activists adopted a nuanced approach, which was mindful of social ties and the trust between individuals, as well as the dignity of those who unwittingly shared falsehoods. The central focus has been on the message, and where possible, its original source – but not the messengers (especially the unwitting ones). Such sensitivity could greatly help in preventing deepening divisions and polarisation, while also promoting a culture of solidarity, collaboration, and civic responsibility in the struggle against disinformation and misinformation.

3.3 Russia's interventions in Georgia

Russia's efforts to undermine Georgia's democratic processes and influence public opinion have long been prevalent, but intensified following the 2008 military aggression and illegal occupation of Georgian territories. Yet military aggression is only one dimension of Russia's efforts to influence the domestic and foreign politics of Georgia. Over the years, Russian disinformation has evolved and adapted, making its activities more covert and difficult to detect. The social media platforms, with fractional monitoring and regulatory frameworks, have become increasingly popular channels for the dissemination and manipulation of content that allowed Russia to further expand disinformation outreach. Limited institutional capacity and unfit strategic communications weaken Georgia's efforts to protect the public information space from Russian interference. Persisting political turbulence, internal disinformation, and the absence of a 'whole-of-society' approach against Russian disinformation all make Georgia particularly vulnerable to ongoing foreign disruptive meddling.

3.3.1 State of play

Despite widespread support for democratisation, Georgians still find it difficult to embrace the fundamental democratic values of diversity and equality[210]. Notwithstanding the solid support (80 %) for Georgia's EU membership aspirations[211], over a third of society still consider the process a threat to Georgian traditions and identity[212]. The alleged incompatibility of Western values with Georgian traditions makes up the central claim upon which Russian disinformation narratives are based. These narratives coincide with the predominant viewpoint of the Georgian Orthodox Church, one of the most trusted institutions in Georgia[213]. Over the years, Russia has effectively exploited this vulnerability of Georgian society using local proxies, political parties, clerics, anti-liberal and ultra-conservative forces, and civic actors to demonise the West and demonstrate it as ethically incompatible with the Georgian value system.

For a number of years, the impact of disinformation was mainly analysed through the lens of the negative effects on public sentiments and perspectives[214]. However, recent developments in Georgia demonstrate that the impact of Russian disinformation goes beyond influencing public opinion and unsettles democratic values and propagates violence. After a March of Dignity was scheduled to take place in Tbilisi on 5 July, pro-Russian outlets Alt-info, Obieqtivi TV, News Front Georgia, Georgia and the World started to disseminate anti-Western narratives (including that the West is 'imposing homosexuality on Georgia'[215]). Media Development Foundation (MDF), a local organisation working on disinformation, identified

[210] Bolkvadze, N., 'How Russia Targets the Cognitive Domain to Achieve its Strategic Goals in Georgia', in 'Georgia's Information Environment through the Lens of Russia's Influence', 2021, NATO Strategic Communications Centre of Excellence, 2021.
[211] NDI 2021, 'Public Attitudes in Georgia: Results of December 2020 telephone survey'. Carried out for NDI by CRRC Georgia, retrieved 20 August 2021,
[212] Lejava, N., 'Georgia's Unfinished Search for Its Place in Europe', Carnegie Europe, 2021.
[213] Gegeshidze, A., Mirziashvili, M., 'The Orthodox Church in Georgia's Changing Society', Carnegie Europe, 2021.
[214] EUvsDisinfo, 'Disinformation Can do Anything: From Insulting People to Ruining Them', 2021.
[215] Ibid.

different actors including political parties, clerics, media, and civil society representatives spreading disinformation, anti-pride, and anti-Western narratives[216]. This was followed by violent demonstrations against Tbilisi Pride's March of Dignity, and numerous victims[217]. During the protests, 55 citizens were attacked. Among them, 53 media representatives were physically assaulted, and TV Pirveli camera operator Lekso Lashkarava allegedly suffered fatal injuries[218].

Among politicians, Levan Vasadze, the head of the political party 'Unity, Essence, Hope', with close ties with the leader of Eurasia Movement Aleksandr Dugin, was one of the prominent figures propagating violence[219]. A Georgian far-right group, Alt-info (which describes itself as a reliable online media outlet and which has close ties to Levan Vasadze), ensured mobilisation of violent groups against the March of Dignity[220]. Alt-info has been removed multiple times on Facebook for the dissemination of anti-Western narratives. In 2020 Facebook removed 130 inauthentic profiles, groups, and pages linked to Alt-info[221]. Following the suspension of the main communication channel on Facebook, the far-right group relocated to encrypted applications[222]. Alt-info's Telegram group, which has over 2,000 members, as well as its TikTok account, were used to mobilise citizens to storm the offices of two youth-led, pro-democracy organisations, the Tbilisi Pride and the Shame Movement, during the violent protests[223]. Another key actor engaged in dissemination of anti-Western disinformation narratives was Davit Tarkhan-Mouravi, the leader of the Alliance of Patriots of Georgia. According to an investigation by the Dossier Center, the party was financed by Russia and has served Russia's interests[224]. The Alliance of Patriots-owned television channel TV Obieqtivi was among the most prominent media sources spreading anti-pride and anti-Western narratives[225].

Based on open-source analysis, the Atlantic Council's Digital Forensic Research Lab (DFRlab) did not find direct Russian involvement; however, actors behind the July 5th violent protests have a record of affiliation with Russia[226]. On the day of the protest, Alexandr Dugin's Facebook posts shared Alt-info's content praising violent groups for 'changing the world balance to Russia's benefit'[227]. In line with a targeted suppression of minorities and the violence on media representatives, violent groups also incited the burning of the EU flag. According to DFRlab analysis, this action goes beyond mobilisation of domestic groups and rather resembles a well-organised action against 'LGBT community, civil society organisations (CSOs), western embassies, and Georgia's Euro-Atlantic aspirations in general'[228]. This was reflected in the joint letter of EU Delegation and 24 Member State embassies addressed to the Government of Georgia assessing this act as a 'direct attack on Georgia's democratic and pro-European aspirations'[229]. Despite the evidence and continuous protests of journalists, civil society and the public, victims of violent protests are still waiting for those responsible to be punished in accordance with Georgia's legislation[230].

[216] Kistauri, A., Kintsurashvili, T., Khutsishvili, K., ' Radicalization in the Name of Religion and against Political Opponents – by whom and what Reason is the Pride March used for?', MythDetector, 2021.
[217] EUvsDisinfo, 'Pro-Kremlin Outlets as Amplifiers of Hate Speech in Georgia', 2019.
[218] Ibid.
[219] Gelava, S., Buziashvili, E., 'Online calls for attacks against Georgia's LGBTQ community result in offline violence', DFRlab, 2021.
[220] Ibid.
[221] Gigitashvili, G., Leroux, J., 'Facebook removes inauthentic assets connected to Georgian far-right group Alt-Info',DFRlab, 2020.
[222] Autor's interview with Givi Gigitashvili, Atlantic Council's DFRlab, 25 August 2021, via MS Teams.
[223] Gelava, S., Buziashvili, E., op. cit., 2021.
[224] Kiparoidze, M., Patin, K., 2020, 'Investigation alleges Russian money behind political party in neighboring Georgia', codastory.com.
[225] Kistauri, A., Kintsurashvili, T., Khutsishvili, K., op. cit., 2021.
[226] Gelava, S., Buziashvili, E., op. cit., 2021.
[227] Ibid.
[228] Ibid.
[229] Official Twitter account of the EU Ambassador to Georgia, Carl Hartzell.
[230] Civil Georgia, 'July 5 Violence Organizers Not Identified, Ombudsperson Says', 2021.

Pre-election disinformation campaigns

Pro-Russian media outlets were actively used for disinformation purposes ahead of the 2020 Parliamentary elections in Georgia[231]. Following an analysis of open sources, Facebook abolished personal accounts and groups engaged in inauthentic coordinated behaviour circulating Sputnik and News Front content. While accounts affiliated with News Front-were 'instigating antagonism and aggression among Georgian Facebook users', fake accounts linked with Sputnik disseminated content that was not political and mostly of sensational ("yellow") nature, aimed at attracting followers[232]. Such a subtle or indirect approach might be driven in part by the public's unfavourable attitude towards openly pro-Russian politics – something that was amply demonstrated by the mass anti-occupation protests that were triggered by the presence of a Russian MP in Tbilisi in June 2019. MDF's pre-election monitoring further revealed the dissemination of anti-Western disinformation narratives by political parties affiliated with Russia, such as the Alliance of Patriots of Georgia and Georgian March[233]. Political parties were manipulating history and spreading Russian disinformation narratives. One of the most prominent cases was Davit-Gareji. Disinformation stories linked to the Davit-Gareji issue endeavoured to portray Azerbaijan occupant along with Russia[234].

Weaponisation of mal-information

Russia often exploits mal-information (i.e. information obtained through hacked databases, e-mail accounts, and other sources of information) in Georgia. One of the most serious cases of such cyber disruptions are attacks on the Richard Lugar Centre for Public Health Research. The Lugar Lab is a facility of the National Centre for Disease Control and Public Health (NCDC) in Georgia. The laboratory was the target of Russian disinformation long before the COVID-19 pandemic and featured in disinformation stories that alleged that the US was developing a biological weapon against Russia in Georgia[235]. Attacks on the laboratory increased during COVID-19, given the essential role of the facility in the management of the pandemic[236]. According to MDF, in May 2020 a Kremlin-affiliated Bulgarian journalist, Dilyana Gaytandzhieva, published an article containing documents leaked during the cyber-attack in 2018. She accused the Lugar Lab and Georgian military biologists of being engaged in COVID-19 research since 2012 with US financial assistance and of creating biological weapons. The news was originally published on a journalist's blog, but soon the material featured in Georgian online media sources[237].

Other instances of disinformation in Georgia have focused on the pandemic. The report 'Infodemic in Georgia' (which was based on monitoring traditional and online media sources during the COVID-19 Pandemic), revealed that Russian state news agency Sputnik and Georgian-language media outlets (Georgia and World, News Front Georgia, tvalsazrisi.ge, Sakinformi, and Obieqtivi TV) have spread disinformation and conspiracy theories concerning the pandemic portraying it as man-made, to establish the 'new world order' and 'digital dictatorship'[238]. Sputnik's disinformation also worked to convince people of the superiority of Russia's vaccine, with stories that suggested that Western vaccines ineffective and unreliable, and that the Russian one had been excluded on political grounds[239].

[231] Gigitashvili, G., 'Information operations and the 2020 Georgian parliamentary elections', New Eastern Europe, 2021.
[232] Rizhamadze, N., Russian Information Operation in Georgia – Sputnik's Coordinated Network on Facebook, ISFED, 2020.
[233] Kintsurashvili, T., 'Pre-Election monitoring: Anti-Western Messages, Hate Speech, Fake news', Media Development Foundation, 2020.
[234] Ibid.
[235] EUvsDisinfo, 'DISINFO: US Prepares Biological Weapons Against Russia', 2019.
[236] EUvsDisinfo, 'DISINFO: Suspicious American Military Activity in Lugar Lab, 2020.
[237] Myth Detector, 'How did official documents leak and what experiments are Georgian scientists carrying out on bats?', 2020.
[238] Kintsurashvili, T., 'Infodemic in Georgia', Media Development Foundation, 2020.
[239] Ibid.

Disrupting state institutions

The joint investigation of the government of Georgia, the US, and the UK concluded that in October 2019, the Russian General Staff Main Intelligence Directorate (GRU) Main Centre for Special Technologies (GTsST), also known as Sandworm, performed a massive cyber-attack on Georgia[240]. More than 2,000 Georgian government and privately-run websites were hacked, including court websites containing case materials and personal data[241]. In addition, the broadcasting of at least two private television stations was interrupted. The Georgian population was directly affected by this highly disruptive cyber-attack, while the operation also had the wider effect of sowing insecurity amongst the public and undermining the functioning of democratic institutions[242]. To promote its narrative of the event, Russia launched a follow-up disinformation campaign using multiple channels including official diplomatic service and Russian-backed media outlets[243]. Russia responded to the allegations with official diplomatic denial of responsibility of carrying out cyber-attack, and accused Georgia and the West of Russophobia. The strategy of spreading the same narratives through different communication channels is based on the assumption that readers are more likely to assume that the information is credible if different information sources spread it, which is one pinpoint tactic of Russian disinformation[244].

3.3.2 Georgia's response

Although Russian disinformation in Georgia's public information space has long been prevalent, the government only formally acknowledged the threat in 2017/2018[245]. Even then, a rather limited number of initiatives took shape at the legislative and executive levels to increase state and societal resilience against Russian interference and enhance the country's institutional capacity to deal with it.

In 2018, the Georgian government announced the set up of strategic communication units in all ministries, under the government's coordination. The stated aim was to form an effective and coordinated strategic communications system in the country and reduce the impact of anti-Western disinformation[246]. Although strategic communications units are tasked with using social media as a tool for exposing and countering disinformation, in practice some official pages of these units contain more posts analysing critical media outlets' content than instances of Russian disinformation[247]. Notwithstanding such shortcomings, an important positive asset to the state's strategic communications arsenal is the Information Centre on NATO and the EU that functions under the Ministry of Foreign Affairs. The Centre implements diverse projects and information campaigns, including face-to-face meetings in regions to raise public awareness about Georgia's Euro-Atlantic integration and mitigate anti-Western propaganda.

In February 2019, the Parliament of Georgia launched a thematic inquiry group on disinformation that included representatives of political parties and civil society to discuss the most relevant channels and actors of anti-Western disinformation and work on ideas to better mitigate existing challenges[248]. The formation of the inquiry group has been widely acknowledged by civil society actors as a positive step

[240] Pompeo, M. R., 'The United States Condemns Russian Cyber Attack Against the Country of Georgia', 2021.
[241] BBC.com, 'Georgia hit by massive cyber-attack', 2019.
[242] Press release, Foreign & Commonwealth Office, 'UK condemns Russia's GRU over Georgia cyber-attacks', 2020.
[243] Gigitashvili, G., 'Russia's 2019 cyberattack against Georgia was followed by a full-spectrum propaganda effort', New Eastern Europe, 2020.
[244] Ibid.
[245] Sirbiladze, I., 'Russian Disinformation Campaigns in Georgia: A Study of State and Civil Society Response', PMC Research Center, 2019.
[246] Tsitsikashvili, M., 'Comparing Lessons Learned from Countering Russian Disinformation in Georgia and the Czech Republic', Kremlin Watch Program 2019, 2020.
[247] Tsitsikashvili, M., 'Georgia's Strategic or Partisan Communications?', Factcheck.ge
[248] Parliament of Georgia, 'Nino Goguadze Introducing the Report of the Thematic Inquiry Group on Disinformation and Propaganda', 2020.

forward. However, the Georgia Reforms Associates (GRASS), one of the organisations working on Russian disinformation, documented shortcomings within the inquiry's working process, including limited engagement of civil society representatives and insufficient participation of key ministries, such as the Ministry of Foreign Affairs, the Ministry of Education, Science, Culture and Sport of Georgia, and the State Security Service of Georgia[249].

In May 2019, the parliamentary faction of the Movement of Liberty-European Georgia presented a legislative package aimed at pushing back against Russian propaganda at the legislative level. A legislative initiative was developed in cooperation with civil society organisations and field experts.

The draft included several important legal proposals prohibiting the Georgian government from funding, making purchases, or otherwise directing budget funds to organisations that oppose Georgia's European and Euro-Atlantic integration, and banning the government from funding organisations (including media) disseminating Russian propaganda messages in Georgia, specifically those that undermine the territorial integrity of Georgia[250]. The proposal was not discussed due to the lack of political will of the ruling Georgian Dream party[251]. This was the second time a proposed law failed to progress: in 2017, Transparency International (TI) Georgia unsuccessfully pushed a package of legislative amendments against Russian propaganda with steps to prohibit political advertisements and election campaign comprised of narratives threatening the sovereignty and territorial integrity of the country[252].

Civil society has an essential role in combatting the malign impact of disinformation on democratic processes. In Georgia, CSOs working on the issue of disinformation have swiftly adapted to the fast-changing challenges of digital space and effectively integrated social media monitoring into their programmes. Civil society's counter-disinformation efforts cover all three dimensions (actors, behaviour, content) of the ABC framework that is often used for analysis and assessment of counter-disinformation activities[253].

Table 1: Three-dimensional framework for analysing disinformation

Actors	Detecting and exposing actors engaged in disinformation
Behaviour	Analysing disinformation actors' behaviour, displaying coordinated and inauthentic behaviour
Content	Analysing and assessing the clout of disinformation

Source: Author's compilation based on works of C. François and J. Pamment[254]

Specific initiatives include[255]:

- Myth Detector/Media Development Foundation (MDF): Myth Detector is MDF's fact-checking and myth debunking platform, which has been operating in five languages since 2014. The planform is aimed at raising the awareness of citizens and institutions in Georgia about the influence of disinformation. Since 2016, MDF has collaborated with EUvsDisinfo. While since 2020 Myth Detector also partners with Facebook to review the accuracy and authenticity of content[256]. MDF

[249] Georgia's Reforms Associates, Statement on the Process of Drafting and the Final Report of the Thematic Inquiry Group on Disinformation and Propaganda', 2020.
[250] Tabula.ge, 'European Georgia presents legislative package aimed at mitigating Russian propaganda', 2019.
[251] Sirbiladze, I., op.cit., 2019.
[252] Ibid.
[253] François, C., 'Actors, Behaviors, Content: A Disinformation ABC Highlighting Three Vectors of Viral Deception to Guide Industry & Regulatory Responses', Transatlantic Working Group, 2019.
[254]François, C., op.cit, 2019. See also, J. Pamment, 'The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework', Carnegie Endowment for International Peace.
[255] The list is not exhaustive and covers only key initiatives.
[256] Myth Detector, About Myth Detector - MDF's fact-checking platform.

produces multiple reports documenting actors and key sources of anti-Western disinformation in Georgia and serves as an important database on how disinformation narratives, tactics, methods and actors have evolved and adapted[257].

- FactCheck.ge/Georgia's Reforms Associates GRASS: FactCheck Georgia is a media project run by GRASS[258]. FactCheck scrutinises information transmitted through social media networks and media outlets, and provides the public with verified information. Fighting against Russian propaganda features among the main objectives of this organisation[259]. GRASS documents Russian disinformation in Georgia through multiple research reports. GRASS's bi-monthly report, DIsinfoMeter, offers analysis of trends and the scale of the pro-Russian and ani-Western disinformation in Georgia[260]. FactCheck Georgia is a verified member of International Fact-Checking Network (IFCN) since 2017 and partner to Facebook's Third-Party Fact-Checking Program since September, 2020.
- The Atlantic Council's Digital Forensic Research Lab: The Atlantic Council's Research Lab exposes disinformation and fake news. DFRlab documents and analyses instances of disinformation and tries to build digital resilience. DFRlab has assessed pro-Russian narratives and coordinated inauthentic behaviour of groups affiliated with Russia[261].
- International Society for Free Elections and Democracy (ISFED): The ISFED undertakes social media monitoring. ISFED has played a major role in the identification of coordinated and inauthentic behaviours on social media and the removal of inauthentic pages, accounts, and groups on Facebook disseminating pro-Russian and anti-Western narratives. Most importantly, ISFED conducts analysis and debunking of disinformation instances during election periods.
- Transparency International (TI) Georgia: TI and the coalition for Euro-Atlantic Georgia brought together over 20 civil society organisations, and conducted the public information campaigns #GEtner[262] and #StrengthisinEurope, which included multiple activities including meetings in regions of Georgia aimed at mitigating anti-Western disinformation. Most importantly, the campaign included a bi-weekly TV slot, #StrengthisinEurope, which showcased anti-Western disinformation cases followed by informed discussion to demonstrate the conformity of Georgian culture and traditions with Western values[263].
- The Georgia Information Integrity Program: In 2020, the United States Agency for International Development (USAID) launched a new program aimed at helping Georgia building societal resilience against disinformation. The project brings together a number of civil society organisations working on disinformation and seeks to identify new actors in the process of fighting disinformation, and studies what the experiences that make people vulnerable are, and how to address their root causes [264].

The overview of selected specific examples demonstrates that civil society effectively works across the three-dimensional framework and implement projects to document the main actors of disinformation, reveal inauthentic coordinated behaviour, and analyse the content and main narratives of disinformation stories. However, interviews with civil society representatives pointed to the lack of an integrated methodology to measure the impact of disinformation[265]. The development of such a methodology would help both state and civil society actors to target their activities, focusing on the most significant forms of disinformation.

[257] Official website of Media Development Foundation, Researches and Reports: www.mdfgeorgia.ge/eng/research/
[258] FactCheck.ge, About us.
[259] Ibid.
[260] Georgia's Reforms Associates (GRASS), Research: https://grass.org.ge/en/skhva-publikatsiebi/research-157
[261] Interview with Givi Gigitashvili, *op.cit.*
[262] Official Website of coalition for Euro-Atlantic Georgia: www.europeforgeorgia.ge/home-page/
[263] '#Strength is in Europe', Advancing CSO Capacities and Engaging Society for Sustainability (ACCESS), 10 October, 2017.
[264] Interview with Mikheil Benidze, Chief of Party Zinc Network Georgia.
[265] Interview with G. Gigitashvili op. cit. and M. Benidze op.cit.

3.3.3 Conclusions and lessons learnt

The Georgia case demonstrates that the impact of Russian disinformation in Georgia goes beyond influencing the public opinion and propagates violence against pro-democracy actors and democratic values in the country. Russian disinformation in Georgia not only has a deleterious effect on society in general, but has particular targets and victims. The disinformation narratives spread by pro-Russian groups show that the West (the EU and the US) is the main target, and pro-democracy actors (civil society representatives, activists, LGBTI community, journalists, members of opposition political parties) are the main victims, punished for embracing democratic values and Georgia's Euro-Atlantic integration process. The main lesson drawn is that the impact of disinformation can be even larger than influencing public opinion, and can swiftly transform from online narratives to offline violence.

The EU, together with other Western allies, should emphasise supporting the victims of disinformation. Particularly when human rights are violated, the EU can defend and uphold them. This could be dome through the newly adopted Global Human Rights Sanctions Regime developed for dealing with 'serious human rights violations and abuses worldwide', as well as through the engagement of the EU Special Representative for Human Rights[266]. In the case of Georgia, this would also mean to fully investigating the 5 July 2021 protests by Georgian authorities and ensuring that those responsible are punished. The lack of justice and lawful follow-up further incites anti-democracy actors by creating an atmosphere of impunity. The violence against journalists is a tangible attempt to silence critical voices and restrict the freedom of speech and expression – central values for democracy. Based on experience drawing from similar cases of violence (including physical) against the media, the EU could show its support to journalists. For example, a more positive positioning of the EU in Georgia is important to push back against widespread anti-Western and anti-EU disinformation narratives. To commemorate the camera operator Lekso Lashkarava who lost his life following the July 2021 violent protests, the EU might dedicate the 2021 EU Prize for Journalism in Georgia to his memory. To address the lack of public trust in civil society, EU funding could focus on strengthening the legitimacy of civil society actors in Georgia.

The most recent disinformation cases relate to important developments in the country, such as political crises, election periods, and the COVID-19 pandemic, which have acted as entry points to undermine the functioning of democratic institutions, sow public distrust in democratic processes, and discredit the West. A key lesson to be learnt is that myth-busting activities and awareness-raising campaigns have lacked strong impact in the absence of overarching multi-stakeholder policy, a well-functioning legislative framework, and an oversight body monitoring state policy implementation.

The Georgian government's counter-disinformation policy is in a formative phase[267]. While there is political acknowledgement of the threat, concrete steps aimed at mitigating Russian disinformation influence remain modest. The lesson is that counter-disinformation efforts struggle to be effective where there are major gaps in coordination among state and civil society actors working on disinformation. Due to extreme political tension, the ruling party fails to see the opposition political parties and civil society representatives as partners, even on overarching national security issues. Examples of neglected legislative initiatives are tangible illustrations of the absence of a multi-stakeholder approach, which ultimately results in lack of substantive advances in the main law-making body and the functioning legislative framework against Russian disinformation. The launch of the thematic Inquiry Group on Disinformation and Propaganda in the Georgia's parliament, and the subsequent elaboration of a report analysing existing threats and initiating recommendations for executive and legislative branches, is a positive step forward. Yet, Georgia's experience shows that shortcomings flowing from the limited presence of relevant ministries and state agencies in a fully inclusive manner weaken the inclusiveness of counter-disinformation measures.

[266] Council of the European Union, Global Human Rights Sanctions Regime,7 December 2020.
[267] Sirbiladze, I., opt. cit., 2019.

Although the report calls for a clearer, more proactive and coordinated Government policy against disinformation and for an enhanced role for the country's parliament, it lacks specific recommendations on necessary changes in legislation and an acknowledgment of the Parliament's ultimate oversight function over the policy implementation process. To address these shortcoming, domestic actors, in cooperation with the EU and other Western partners, need to focus on strengthening Georgia's legislation against malign Russian disinformation. This legislation should be based on best European practices (including in EU Member States, e.g. Slovakia, Estonia).

Across the three-dimensional ABC framework (described above, in Section 3.3.2), civil society actors' work is commendable in all dimensions. CSOs effectively analyse and document the main actors of disinformation, reveal and fight against inauthentic coordinated behaviour, and analyse the content and its main narratives. However, this study has revealed that civil society faces difficulties in expanding the scope of its activities due to a lack of financial resourses and dependence on donor funding. Furthermore, CSOs' investigative analyses have mostly covered Facebook. The expansion of CSOs' work to other social networks – including (but not limited to) Twitter, Instagram, and TikTok – is necessary. This was particularly evident during the violent protest in July 2021, when pro-Russian groups disseminating disinformation and anti-Western narratives effectively relocated to other social media channels following the removal of inauthentic accounts on Facebook.

While multi-stakeholder policy is necessary to effectively fight disinformation, constant political instability in the country makes it difficult to focus on overarching national security issues. Instances of political manipulation and internal disinformation of both the ruling Georgian Dream and opposition political parties make the fight against external disinformation more challenging.

In light of the analysis, the following specific lessons can be learnt:

1) The lack of a 'whole-of-society' approach limits the effectiveness of civil society's work against the Russian disinformation. A structured coordination framework between state and civil society actors working on disinformation would strengthen the country's counter-disinformation capacity. The development of a functioning legislative framework is of utmost importance, since its absence limits the impact of counter-disinformation activities.

2) The lack of resources of civil society actors allows for only partial coverage and monitoring of Russian disinformation. The Georgia case study demonstrated that social media channels other than Facebook, including encrypted applications, were effectively used to disseminate disinformation. Increased donor support to civil society would strengthen the capacity and allow civil society actors to enlarge the scope of their counter-disinformation activities, including on media literacy programs.

3) Cooperation with social media companies and conglomerates has proven to have beneficial outcomes in the fight against disinformation. A number of civil society actors in Georgia (section 3.3.2) are verified members of the International Fact-Checking Network (IFCN) and act as Facebook's third-party fact-checking organisations. These partnerships have played an essential role in takedowns of hundreds of inauthentic pages on Facebook, spreading disinformation and anti-Western narratives.

4) While the focus of civil society is on external disinformation, the Georgian case study demonstrates that local actors act as amplifiers of disinformation. Instances of internal disinformation and manipulation of content for political purposes make it particularly difficult to mobilise resources for counter-disinformation measures against external sources of disinformation.

5) There is no integrated methodology to measure and analyse the actual impact of Russia's disinformation. The absence of such a methodology limits the effectiveness of counter-disinformation activities, as state or civil society actors are unable to focus their work on target

groups and particular aspects of disinformation. The development of such methodology in collaboration with international experts would facilitate focusing counter-disinformation efforts on the most impactful forms and sources of disinformation, as well as on the most vulnerable targets.

6) Counter-disinformation activities largely depend on fact-checking and myth-busting, predominately communicated to the public through online means. While presenting verified and reliable information is crucial in the fight against disinformation, stronger emphasis should be placed on reaching audiences with limited or no access to the internet. The campaign (discussed earlier) that affected a television programme is a worthwhile example to be taken into consideration while mapping counter-disinformation activities, especially because the majority of Georgian citizens receive information from TV.

7) The limited cyber-security capacity of Georgia exposes the country to foreign disinformation. Russia effectively weaponised information gained through cyber-attacks to develop disinformation stories featuring the email correspondence of Georgian officials. Strengthening Georgia's cyber security capabilities, particularly by reinforcing the protection of critical infrastructure, will contribute to the country's enhanced resilience to cyber-attacks and mal-information.

4 Analysis of the EU disinformation response

The EU has a wide policy toolbox at its disposal, including diplomatic, political, human rights-related and development-focused instruments which can be applied to disinformation. In order to help to counter the spread of disinformation, the EU supports independent media in third countries, engages with civil society, conducts diplomatic activities and spreads positive, fact-based communication. Given the limited length of this report, in this chapter we provide an analysis of those initiatives that deal primarily with disinformation. They have been listed in Table 2 and described in more detail in Annex 2.

Table 2: Disinformation-focused instruments

Disinformation-focused EU instruments
• The East StratCom Task Force and its EUvsDisinfo campaign established in 2015, plus the Western Balkans and South StratCom Task Forces and disinformation-oriented data analysts in the EEAS. • The EU Code of conduct on countering illegal hate speech online, established in 2016, and signed by numerous major social media platforms in the years since. • The European Commission's and EEAS's Action Plan Against Disinformation from 2018. • The Rapid Alert System (RAS) set up among EU institutions and Member States to enable smooth data sharing and alerts on disinformation threats. • The Code of Practice on Disinformation, initiated by the Commission and signed by online platforms including Facebook, Google, and Twitter. • The 2020 European Democracy Action Plan (EDAP). • The 2020 Digital Services Act. • The European Digital Media Observatory (EDMO). • European Parliament's Special Committee on Foreign Interference in all Democratic Processes in the EU (INGE).

Most of the EU instruments presented in the table target the potential consumers, targets, and vectors of disinformation. They are aimed at documenting disinformation cases, raising awareness, and analysing (EUvsDisinfo) and alerting parties about such cases (RAS). They target social media platforms as the main vector through which disinformation spreads (Code of Practice and DSA); and support fact-checkers, researchers, and media that combat disinformation (2018 Action Plan, EDAP, EDMO).

What is lacking are instruments that target information aggressors, those who deliberately spread disinformation and build and support the ecosystems for its spread. In the first place, that would be state actors such as Russia, China, or Iran. Secondly, it could be 'domestic' EU actors and other politicians who regularly spread false information[268]; and finally, private actors, or 'disinformers for hire'[269]. All these players are active not only on social media, but also in traditional media. They often target local influencers who can reach significant audiences, even without automated activity, on social media. The tendency to blur the source of disinformation and find local actors who would spread disinformation for the real perpetrator has been described both in Europe and overseas[270]. These seemingly 'domestic' or 'organic' sources of disinformation will remain untouched by measures targeting fake accounts or automated behaviour, nor will they be covered by initiatives encompassing only disinformation campaigns by external actors.

[268] See e.g. Nielsen, N., & Zalan, E., EU says Orban's new national poll contains 'fake news', EU Observer, 2020; Nardelli, A., and Silvermann, C., Italy's Most Popular Political Party Is Leading Europe In Fake News And Kremlin Propaganda, Buzzfeed, 2016; or the Kremlin's Trojan horses series: Polyakova, A., The Kremlin's Trojan Horses 3.0. Atlantic Council, 2018.

[269] Fisher, M., Disinformation for Hire, a Shadow Industry, Is Quietly Booming, New York Times, 2021.

[270] Kalenský, J., A Change of Tactics: Blurring Disinformation's Source, disinfoportal.org, 2019.

Currently, there are no instruments in place that would discourage Moscow, Beijing, or any other information aggressor from their malicious activities. They face no undesired consequences for their disinformation campaigns. That means that they merely need to adapt to the EU's, Member States', and civil society's defensive measures, which they are already doing. As an example, in 2019, after the EU started highlighting the disinformation activities of official Russian-state pseudomedia, and after social media companies started countering 'coordinated inauthentic behaviour', Russia increasingly focused on spreading pro-Kremlin disinformation via channels that appeared authentic and domestic. These channels were not targeted by measures focusing on inauthentic behaviour and official foreign-state media[271]. In this and other similar cases, the sources of disinformation are free to continue with their campaigns.

The EDAP foresees instruments that would impose costs on perpetrators. This would allow the EU to focus not only on (potential) consumers of disinformation and vectors through which disinformation spreads, but also on the aggressors who deliberately create and spread disinformation. However, concrete measures have yet to be seen. One of the possible instruments would be sanctions against notorious disinformers, be it individuals (such as the already sanctioned Dmitry Kiselyov), or organisations. Sanctioning the disinformation-oriented quasi-media, such as Russian state-owned TV channels, would also result in losses from advertisement revenue – pulling the advertisements of EU-based companies from the disinformation-oriented media would be another form of imposing costs on perpetrators. Organisations and individuals spreading disinformation could also be denied access and cut off, with no accreditations, no access to press conferences, and no answers to their questions. Asymmetric measures are also a possibility[272].

With regards to punitive measures, it seems that the EU is also lacking with respect to investigating malicious information operations. The various US investigations into Russian interference in the 2016 Presidential elections led to criminal consequences, just as Russian interference in the 2020 Presidential elections resulted in sanctions[273]. The US intelligence community is already investigating Russian influence into the (future) 2022 elections[274]. In contrast, the EU does not investigate similar incidents happening in the EU[275]. Without proper investigation, it is almost impossible to identify and justly punish the perpetrators of malicious information operations. In fact, investigations could be conducted at the EU level by special committees in the European Parliament, or by EU Intelligence Analysis Centre (INTCEN), as well as by the Member States and local authorities (interior ministries, security services, parliamentary committees, etc.).

Furthermore, the EU lacks dedicated monitoring and exposing of Chinese disinformation campaigns in a manner similar to EUvsDisinfo, a gap that was also addressed by the INGE Committee in May 2021[276], as well as by MEP Anna Fotyga in Parliamentary Questions[277]. In a similar manner, it would be highly useful to have dedicated teams focusing on systematic, ongoing, day-to-day documentation, exposing and analysing disinformation campaigns with regards to other actors, be they foreign or domestic. While

[271] Kalenský, J., A Change of Tactics: Blurring Disinformation's Source, disinfoportal.org, 2019. See also: Snegovaya, M. & Watanabe, K., The Kremlin's Social Media Inside the United States: A Moving Target, Free Russia Foundation, 2021.

[272] See e.g. Helmus, T.C. & Kepe, M., op. cit., 2021; or Polyakova, A., Fried, D., Democratic Offense Against Disinformation, CEPA, 2020.

[273] U.S. Department of Treasury, Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections, 2021.

[274] Williams, K. B., Bertrand, N., Marquardt, A., New intel reports indicate fresh efforts by Russia to interfere in 2022 election, CNN, 2021.

[275] Kalenský, J., The US Investigations Highlight Europe's Laxity on Disinformation, disinfoportal.org, 2019.

[276] https://www.europarl.europa.eu/doceo/document/O-9-2021-000035_EN.html.

[277] Fotyga, A., Priority question for written answer P-002103/2020 to the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy, 2020.

researchers, think tanks, and civil society organisations do a lot of work in this regard, they do not have the resources and the 'big picture' perspective to monitor disinformation incidents throughout the EU in a systematic, exhaustive, and ongoing manner. At least so far, there have been no visible products in this regard coming out of EDMO and the supported initiatives.

Thus, the EU still lacks authority that would provide EU citizens (and other EU institutions) with comprehensive information on how many disinformation incidents there are in the EU on a daily basis, how many actors are involved, how many people are targeted, and how many are actually persuaded[278]. Both the Action Plan from 2018 and EDAP mention the need to better detect and expose disinformation campaigns, but there does not seem to be any other initiative, apart from the EUvsDisinfo campaign (which is currently limited to one specific actor), doing that on a systematic and regular basis so far.

The RAS connects the Member States with EU institutions and should enable prompt reaction to newly emerged disinformation incidents. It could thus be a perfect instrument for rapid alerts among the Member States and EU institutions. However, it does not seem to deliver on this promise[279]. Even 18 months after its announcement, the Commission still acknowledged that the EU would benefit from a faster and more coordinated response, and asked that the Member States use the RAS more extensively[280], which shows room for improvement. While the RAS could work in theory, as mentioned above and also in the European Court of Auditors report[281], it does not fulfil this function in reality, since the Member States' representatives do not add alerts about newly emerging disinformation incidents in their countries. In such circumstances, it is worth considering other actors which could get involved. Perhaps representatives from civil society, monitoring the disinformation landscape in their countries, would be more diligent in adding such alerts.

Finally, many EU documents dealing with disinformation mention the need to better coordinate efforts with regards to disinformation. Currently, different aspects of the problem are addressed by various institutions (the EEAS and the European Commission's DG CNECT, DG COMM, and Vice President for Values and Transparency). For better coordination, it might be useful to consider establishing a dedicated EU agency dealing with disinformation. Such a body could concentrate all the EU work on disinformation in one institution. A similar agency (focusing only on foreign disinformation) is currently being built in France under the Prime Minister's authority[282].

Given political sensitivities, it is also possible to consider a division of labour where foreign disinformation would be covered by the EU and Member States, while domestic disinformation would be covered by civil society. In such a case, the model of 'Transparency International for Disinformation'[283], which would systematically deliver comparable data from target countries, seems to be ideal. Transparency International (TI) has regional offices that deliver the same data to the TI hub. It is, therefore, possible to compare the levels of corruption in the countries covered by TI and issue regular reports showing the trends and development in time. Having a similar model for disinformation (instead of corruption) would enable the EU to compare data related to disinformation from target countries, something currently unavailable. This model would provide answers to some of the unanswered questions mentioned above, e.g. on the number of disinformation incidents, actors, vectors, as well as the success rate, etc.

[278] The need to address these and other similar questions was mentioned by researchers already right after the 2018 Action Plan: Kalenský, J., Freudenstein, R., The EU's Action Plan Against Disinformation: Good First Step, Now We Need a Follow-Up, disinfoportal.org, 2018.
[279] Emmott, R., Carbonnel, A. D., Humphries, Who burned Notre Dame? Brussels goes after fake news as EU election nears, Reuters, 2019.
[280] European Commission & HRVP, Tackling COVID-19 disinformation - Getting the facts right, JOIN(2020) 8 final of 10 June 2020.
[281] European Court of Auditors, Disinformation affecting the EU: tackled but not tamed, 2021.
[282] Vilmer, J.-B., Effective state practices against disinformation: Four country case studies, Hybrid Center of Excellence, 2021.
[283] An earlier idea of Peter Pomerantsev and Michael Weiss: Pomerantsev, P., Weiss, M., The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money, 2014.

5 Conclusions and lessons learnt

The EU has instruments in place that focus on the consumers, targets, and vectors of disinformation. What is lacking, however, are instruments that target those who deliberately produce and spread disinformation. Apart from that, it would be useful to consider how to also cover non-Russian disinformation players in a manner similar to EUvsDisinfo, and how to improve the coordination of the various initiatives and countermeasures against disinformation, e.g. via a new dedicated agency.

The Iranian case study shows that Iran is among the actors who focus on 'laundering disinformation' through seemingly legitimate front and proxy media. These operations will remain untouched by measures targeting fake accounts or inauthentic behaviour.

They could be exposed (although not stopped) by a dedicated Task Force focusing on this particular actor and their tactics. Fact-checkers and investigative journalists could also help with this task on a regular basis, if adequately funded and motivated to focus on this topic. Sanctions against those who propagate falsehoods would be helpful to introduce consequences for such a behaviour, and make clear that it is not accepted, but sanctions would have to be proceeded by appropriate investigations in order to identify those who should be sanctioned.

The Chinese operations directed against Taiwan used a network of inauthentic accounts. However, shutting down of thousands of these accounts did not break the network. Some of the disinformation content is also amplified by the legitimate accounts of Chinese officials, and by domestic Taiwanese actors – a fact that blurs the 'external vs. domestic' distinction. This kind of amplifying activity could also be exposed by a dedicated Task Force or civil society actors. Taiwan also has legal measures sanctioning certain types of disinformation (e.g. about epidemics, natural disasters, or product quality) and political activities coordinated by a foreign power. However, these measures are also criticised as threatening freedom of expression, which would make their transfer to the EU impossible. Apart from that, the government focuses on prompt, viral, and humorous pre-emptive counter-campaigns based on real-time assessment of the social media trends (thereby helping to prevent disinformation from penetrating large and traditional media outlets), supporting local civil society actors countering disinformation, and on media literacy programs in the school curricula.

The Russian operations against Georgia use a variety of channels to deliver the desired message: official Russian media, other pro-Russian outlets, social media, encrypted messengers, and local pro-Russian actors. Some of these operations have been documented and exposed by the EUvsDisinfo campaign and its local partners, and by other civil society actors in the country. However, going beyond identifying and exposing disinformation seems currently impossible for Georgia's civil society actors given their insufficient resources. The country's response is further weakened by the absence of a 'whole-of-society' approach (cooperation between the government and civil society actors does not seem to be working) and the heavily polarised political situation in the country. Information Centre on NATO and EU, functioning under the MFA, focuses on campaigns mitigating Anti-Western disinformation and similar work is being done by the local civil society actors. The malicious information operations by (pro-)Russian actors in Georgia have gone beyond 'just' influencing public opinion to result in violence, which shows that the impact of current counter-disinformation efforts seems to be limited.

Based on the analysed case studies and the lessons drawn locally, the EU can learn the following lessons:

1) Disinformation actors use a wide range of channels, including apparently independent websites and front media without a visible connection to the disinformation actors (*Iran, Lesson 1*). External disinformers frequently use local actors and enablers to deliver their messages (*Taiwan, Lesson 1*), and also manage to outsource their disinformation activities to other countries (*Iran, Lesson 3*). They are capable of hiding behind another country's top level domains (*Iran, Lesson 2*). Local nuances and polarisation of societies are also key for understanding the local disinformation environment (*Taiwan, Lessons 2 and 8*).

   Currently, the EU monitors and exposes only Russia's disinformation campaigns in a systematic, regular, and visible fashion. In order to monitor the constantly developing activities and to be able to understand the local specificities with regards to other, non-Russian actors, it is important to establish dedicated actor-specific teams capable of following the most recent disinformation developments and understanding the local environments in which disinformation spreads. The East StratCom Task Force that monitors Russia's disinformation campaigns can serve as an example. However, even Russia's disinformation campaigns are currently monitored only partially (*Georgia, Lesson 2*).

2) There is a significant disparity of resources between disinformation actors on the one hand, and civil society actors countering these activities on the other hand (*Iran, Lesson 5*). Civil society actors lack the resources to monitor, analyse, and counteract disinformation activities (*Georgia, Lesson 2*), and their work is further made harder by domestic political actors using disinformation (*Georgia, Lesson 3*). Governments and EU institutions can help to create a favourable environment for civil society activities countering disinformation and other related activities (*Taiwan, Lesson 3*), including media literacy programs (*Taiwan, Lesson 4*). The disparity of resources can be solved by:

   a. increased support for the civil society;

   b. measures aimed at limiting the activities of the disinformation actors.

3) There is not enough research measuring the impact of disinformation activities (*Iran, Lesson 4 and Georgia, Lesson 4*). This can make civil society's efforts to counter disinformation even more difficult (*Georgia, Lesson 4*).

4) Reliable media that sit behind paywalls and effectively counter disinformation-oriented 'media' have a comparative disadvantage to the outlets focused on spreading disinformation (*Taiwan, Lesson 7*). Stronger support for reliable media outlets from governments or EU institutions in order to reduce their reliance on paywalls could help to correct this imbalance.

5) Proactive campaigns pre-empting and neutralising disinformation in advance (*Taiwan, Lesson 3*) using memes and humour (*Taiwan, Lesson 6*) have proven to be effective in countering disinformation.

6) A 'whole-of-society' approach to countering disinformation helps (*Taiwan, Lesson 3*), whereas its absence limits the effectiveness of counter-disinformation activities (*Georgia, Lesson 1*). It is necessary to better coordinate the various counter-disinformation activities in the EU, both among EU institutions and Member States, and between them and civil society.

6 Recommendations

In order for the EU to be more effective at defending itself against malicious information operations, based on the lessons formulated in Chapter 5, we propose the following recommendations:

- The EEAS and the Commission should introduce instruments similar to the EUvsDisinfo campaign aimed at detection and exposing of disinformation campaigns and raising awareness about them, also covering non-Russian disinformation players (e.g. China, Iran, or domestic EU actors). Alternatively, the domestic actors could be covered by a dedicated CSO, described below in Recommendation 2. In doing so, the EU should extensively use the experiences of the EUvsDisinfo campaign, which also needs to be strengthened – as has been requested a number of times (based on Lesson 1 for the EU).
- The European Commission should take action to ensure it more rapidly and robustly implements measures to support independent media and civil society initiatives countering disinformation within the EU. This means, for example, providing greater financial support to more civil society actors and media countering disinformation, including those focusing on local media literacy programs (Lessons 2a, 3, and 4 for the EU). In order to significantly boost civil society activities countering disinformation and to start collecting comparable data from the EU Member States, and to systematically monitor disinformation actors within the EU (a task that might be too politically sensitive for EU institutions), the EU could initiate the development of a new 'Transparency International for Disinformation'; a dedicated CSO that regularly and systematically delivers comparable data about disinformation campaigns from target countries. This would provide new and valuable data about the number of disinformation incidents, actors, vectors, and channels, and about the success rate of disinformation, as well as trends and development over time (Lessons 1 and 2a for the EU).
- The European Commission, the European Parliament, and the EU Member States should adopt measures that enable the perpetrators of disinformation to be punished and sanctioned, as envisaged in EDAP. This could entail sanctions against individuals and organisations regularly spreading disinformation, cutting them off from advertisement revenue and denying them access to EU institutions (e.g. by not issuing press accreditations, providing no entry to EU institutions and press conferences, not responding to questions). The sanctions adopted in the US following investigations into interference in both the 2016 and 2020 presidential elections can serve as an example (Lesson 2b for the EU). In order to identify the individuals and organisations that should be sanctioned, the EU could consider launching official investigations into disinformation operations, similar to the investigations in the US following the 2016 and 2020 presidential elections. Such investigations could be conducted at the EU level by the INGE (or another) Committee in the European Parliament, by INTCEN in the case of disinformation operations targeting the EU, or by the Member States and local authorities (interior ministries, security services, national parliamentary committees) in the case of disinformation operations targeting the Member States.
- All European institutions and Member States should focus on developing rapid, proactive, pre-emptive campaigns based on real-time assessment of social media trends and topics identified as targets of disinformation campaigns (measures in Recommendation 1 would help to identify these topics), ideally using humour (Lesson 5 for the EU).
- The European Parliament and/or European Commission should consider establishing a new EU agency for countering disinformation to better coordinate the EU's counter-disinformation initiatives. The agency that is currently being built in France under the Prime Minister's authority to counter foreign disinformation can serve as an example. For better coordination between the

EU and Member States, Member States should use the Rapid Alert System more effectively. The EEAS could assist in this, and consider opening this instrument to civil society alerts about disinformation incidents (Lesson 6 for the EU).

Annex 1: Overview of relevant EU instruments

The EUvsDisinfo campaign[284], launched in 2015 by East StratCom, focuses on documenting cases of pro-Kremlin disinformation and raising awareness about them in analytical articles. The approach is actor-specific, and the team focuses on the Kremlin's information channels and the ecosystem replicating the same messages. The focus is more on traditional media (TV, print, and websites) rather than social media. As of August 2021, the EUvsDisinfo database contains over 12,000 disinformation cases, and publishes analytical articles describing the methods, aims, and targets of the pro-Kremlin disinformation campaign on a daily basis. The Western Balkans and South StratCom Task Forces do not have publicly available products of their own.

The **Code of conduct on countering illegal hate speech online**[285] was signed in 2016 by Facebook, Microsoft, Twitter, and Youtube; other platforms endorsed the code in the following years. The companies signed up must 'review the majority of valid notifications for removal of illegal hate speech in less than 24 hours, and remove or disable access to such content, if necessary'. According to the latest monitoring exercise, the companies now assess 90 % of notifications within 24 hours and 71 % of the reported content is removed[286].

In December 2018, the **Action Plan on Disinformation**[287] presented four pillars for a coordinated response to disinformation: (i) improving the capabilities of EU institutions to detect, analyse, and expose disinformation; (ii) strengthening coordinated and joint responses to disinformation; (iii) mobilising private sector to tackle disinformation; and (iv) raising awareness and improving societal resilience. In the first pillar, the Action Plan called for strengthening of the StratCom Task Forces, and for a review of the mandate of Western Balkans and South StratCom Task Forces, to enable them to address disinformation, as well as strengthening of the EU Delegations in order to better detect, analyse, and expose disinformation. The calls for strengthening and stabilisation of the StratCom Task Forces were also repeated by the European Parliament in later years[288], and reiterated in the 2020 European Democracy Action Plan (EDAP)[289]. These repeated calls show that strengthening either has not occurred yet, or has not been sufficient so far (which was also confirmed by the auditors' report in 2021[290]). In the second pillar, the Action Plan announced the establishment of the **Rapid Alert System (RAS)**, 'set up to provide alerts on disinformation campaigns in real-time'. In the third pillar, the document highlighted the Code of Practice on Disinformation, and called upon all signatories to swiftly implement the actions and procedures identified in it. The Code will be discussed later. Finally, in the fourth pillar, the Action Plan called upon the Member States to 'support the creation of teams of multi-disciplinary independent fact-checkers and researchers with specific knowledge of local information environments to detect and expose disinformation campaigns across different social networks and digital media', and promised continued support of independent media, quality journalism, and research into disinformation. This resulted in the creation of the **European Digital Media**

[284] https://euvsdisinfo.eu/
[285] European Commission, The EU Code of conduct on countering illegal hate speech online, 2016.
[286] European Commission, Countering illegal hate speech online. 5th evaluation of the Code of Conduct, 2020.
[287] European Commission & HRVP, Action Plan against Disinformation, JOIN(2018) 36 final of 5 December 2018.
[288] See for example European Parliament, European Parliament recommendation of 13 March 2019 to the Council and the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy concerning taking stock of the follow-up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda against it by third parties (2018/2115(INI)); European Parliament, P9_TA(2020)0009 Annual report on the implementation of the Common Security and Defence Policy. European Parliament resolution of 15 January 2020 on the implementation of the common security and defence policy – annual report, (2019/2135(INI)); or Fotyga, A., Priority question for written answer P-002103/2020 to the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy, 2020.
[289] European Commission, On the European democracy action plan, COM(2020) 790 final of 3 December 2020.
[290] European Court of Auditors, Disinformation affecting the EU: tackled but not tamed, 2021.

Observatory (EDMO)[291], which recently announced eight national hubs covering 14 Member States plus Norway[292].

The **Code of Practice on Disinformation** was introduced in October 2018[293]. Leading social networks and online platforms agreed with the European Commission on self-regulatory standards to fight disinformation. The Code was signed by Facebook, Twitter, Google, Microsoft, and Tik Tok, among others. The Code's commitments were organised under five pillars: (i) scrutiny of ad placements; (ii) political advertising and issue-based advertising; (iii) integrity of services; (iv) empowering consumers; and (v) empowering the research community.

While the Code was definitely a success in bringing together some of the biggest platforms and making them adhere to unified principles, the first-year assessment also identified numerous shortcomings in the platforms' progress[294]. These were grouped into four broad categories: (i) inconsistent and incomplete application of the Code across platforms and Member States; (ii) lack of uniform definitions; (iii) existence of several gaps in the coverage of the Code commitments; and (iv) limitations intrinsic to the self-regulatory nature of the Code.

In 2021, the Commission presented guidance to strengthen the Code[295]. This guidance aims to evolve the self-regulatory Code towards a co-regulatory instrument foreseen under the Digital Services Act (to be described later). It calls for reinforcing the Code by strengthening it in the following areas: (i) larger participation with tailored commitments; (ii) demonetising disinformation[296]; (iii) ensuring the integrity of services; (iv) empowering users to understand and flag disinformation; (v) increasing the coverage of fact-checking and providing increased access to data to researchers; (vi) a robust monitoring framework based on clear key performance indicators, measuring the results and impact of actions taken by the platforms, as well as the overall impact of the Code on Disinformation in the EU.

The EDAP[297] was presented in December 2020, and also covers promotion of free and fair elections, and support for free and independent media. In the final part, the document outlines measures to counter disinformation, which include: (i) improving EU and Member State capacity to counter disinformation; (ii) more obligations and accountability for online platforms; and (iii) empowering citizens to make informed decisions.

Unlike the previous documents, the EDAP also mentions the need to develop 'new instruments that allow imposing costs on perpetrators'. It also highlights the need to increase cooperation, both within the EU and internationally; to increase support for capacity-building of national authorities, independent media, and civil society in third countries to detect and respond to disinformation and foreign influence operations; to strengthen the Code of Practice (described above); and to support new initiatives fighting disinformation, promoting media literacy and helping citizens to identify disinformation.

[291] European Commission, European Digital Media Observatory (EDMO), 2021 and European Digital Media Observatory, EDMO at a Glance, 2021.
[292] European University Institute, National EDMO hubs announced, 2021.
[293] European Commission, Code of Practice on Disinformation, 2021.
[294] European Commission, Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement, SWD(2020) 180 final of 10.9.2020. See also Plasilova, I. et al., Study for the 'Assessment of the implementation of the Code of Practice on Disinformation'. Final Report, 2020; Pamment, J., EU Code of Practice on Disinformation: Briefing Note for the New European Commission, Carnegie Endowment for International Peace, 2020.
[295] European Commission, Commission presents guidance to strengthen the Code of Practice on Disinformation, 2021.
[296] A measure that was first mentioned in 2018, but still does not seem to be fully implemented: Kalenský, J., Hitting COVID-19 disinfo websites where it hurts: their wallets, medium.com/dfrlab, 2020.
[297] European Commission, On the European democracy action plan, COM(2020) 790 final of 3.12.2020.

The proposal for the **Digital Services Act** (DSA)[298] was introduced in December 2020. It lays down different sets of obligations for different online players depending on their size. The 'very large online platforms' (companies reaching more than 10 % of the EU population, i.e. currently 45 million people, on a monthly basis) have all the obligations of smaller players, plus obligations to manage 'systemic risks', defined in Article 26. The first category of systemic risks covers illegal content (such as child sexual abuse material or illegal hate speech). The second category concerns the impact of the service on fundamental rights, such as freedom of expression and information. The third category of risks concerns the manipulation of the platform's service, e.g. through fake accounts, bots, or automated behaviour.

The platforms should, upon request, provide access to data necessary to monitor compliance with the DSA (Article 31), but this is limited to 'vetted researchers' from academic institutions — this was criticised both due to the limitations of providing data only upon request[299], and only to academia[300].

As mentioned in an earlier report, 'some disinformation content may also be illegal (defamation or incitement to hatred), and thus may be tackled under Article 14 of the DSA'[301]. Notices submitted by 'trusted flaggers' shall be processed with priority (Article 19).

Some researchers think that the risks related to disinformation should be further specified in the DSA[302], and that the definition of 'systemic risks' is too narrow and does not cover many of the tactics that are frequently used by the disinformers, such as information laundering, state-sponsored propaganda, or organic virality[303].

The European Parliament **Special Committee on Foreign Interference in all Democratic Processes in the EU (INGE)** started its work in September 2020[304]. The committee is mandated to 'examine, among others, how outside manipulation and campaign financing affected elections in the EU, and what the EU could do to counter disinformation'.

[298] European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final of 15.12.2020.
[299] Wanless, A., How Europe Can Tackle Influence Operations and Disinformation. Carnegie Europe, 2021.
[300] EU Disinfo Lab, How the Digital Services Act (DSA) Can Tackle Disinformation, 2021.
[301] Bayer, J. et al., Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States. 2021 update. European Parliament, 2021.
[302] EU Disinfo Lab, op.cit.
[303] Cesarini, P., Regulating Big Tech to Counter Online Disinformation: Avoiding Pitfalls while Moving Forward. Media Laws, 2021.
[304] New committees begin their work, European Parliament, 2020.

Annex 2: Bibliography

#Strength is in Europe, Advancing CSO Capacities and Engaging Society for Sustainability (ACCESS), East-West Management Institute, 2017.

20180516 - RightsCon 2018 - cofacts - Google Slides, 2021.

20180516 - RightsCon 2018 - cofacts - Google Slides, 2021.

A Conversation with Audrey Tang, Fondation pour la Recherche Strategique, 2020.

Aghekyan, E., Schafer, B., Deep in the Data Void: China's COVID-19 Disinformation Dominates Search Engine Results, Alliance for Securing Democracy, 5 October, 2021.

Anderson, C. and Sadjadpour, K., Iran's Cyber Threat: Espionage, Sabotage, and Revenge, Carnegie Endowment for International Peace, 2018.

Aspinwall, N., Taiwan President Sues Scholars for Alleging Her Doctorate Degree is Fake, The Diplomat, 2019.

Aspinwall, N., Taiwan's War on Fake News Is Hitting the Wrong Targets, Foreign Policy, 2020.

Associated Press, Cyborgs, Trolls and Bots: A Guide to Online Misinformation, VOA News, 2020.

Barojan, D., #TrollTracker: Bots, Botnets, and Trolls, DFRLab, 2018.

Bayer, J. et al., Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, European Parliament, 2019.

Bayer, J. et al., Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States. 2021 update, European Parliament, 2021;

BBC, Georgia Hit by Massive Cyber-attack, 2019.

Beauchamp-Mustafaga, N. and Drun J., 'Exploring Chinese Military Thinking on Social Media Manipulation Against Taiwan,' China Brief 21/7, 2021.

Bolkvadze, N., How Russia Targets the Cognitive Domain to Achieve its Strategic Goals in Georgia, 2021.

Bontcheva, K. et al, Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression, Broadband Commission for Sustainable Development, 2020.

Bradshaw, S., Bailey, H. and Howard, P.N., Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation, University of Oxford, 2021.

Bradshaw, S., Influence Operations and Disinformation on Social Media, Centre for International Governance Innovation, 23 November 2020.

Bulut, E., Yörük, E., Mediatized Populisms | Digital Populism: Trolls and Political Polarization of Twitter in Turkey, International Journal of Communication, Vol. 11, 2017.

Cesarini, P., Regulating Big Tech to Counter Online Disinformation: Avoiding Pitfalls while Moving Forward, Media Laws, 2021.

Chang, H. et al., 'Digital Civic Participation and Misinformation during the 2020 Taiwanese Presidential Election,' Cogitatio 9/1, 2021.

Chou, B., Taiwan's Proposed Bills To Regulate Online Content Stir Outrage, The News Lens, 2020.

ClearSky, Global Iranian Disinformation Operation, 2018.

Clearsky, Yemen-Based Disinformation Campaign Distributing Fake News in Israel and the Arab World, 2019.

Cofacts Interview Notes [L'Usine Digitale], March 2020.

Cofacts Interview Notes [DW Brazil], July, 2018.

Cofacts Interview Notes [ITS Rio], October, 2019.

Cofacts Interview Notes [Splice], July, 2018.

Cofacts Interview Notes [Taipei Times], June, 2018.

Cofacts Interview Notes [The Diplomat], October, 2018.

Cofacts Interview Notes [TNLi], 2018.

Cohen, R. S., Demus, A., Schwille, M., Vest, N., U.S. Efforts to Combat Foreign Disinformation on Social Media, RAND Corporation, 2021, not available to the general public[1]

Cohen, R.S. et al., Combating Foreign Disinformation on Social Media: Study Overview and Conclusions, RAND Corporation, 2021.

Committee to Protect Journalists, One Country, One Censor: How China undermines media freedom in Hong Kong and Taiwan, 2019.

Cook, S., Beijing Is Getting Better at Disinformation on Global Social Media, The Diplomat, 2021.

Cook, S., Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence since 2017, Special Report, Freedom House, 2020.

Cook, S., China's Global Media Footprint. Democratic responses to expanding Authoritarian Influence, Sharp Power and Democratior Resilience Series, National Endowment for Democracy, 2021.

Crisp, W. and al-Salhy, S., Exclusive: Inside Hizbollah's Fake News Training Camps Sowing Instability Across the Middle East, Telegraph, 2020.

Daniels, R., Taiwan's Unlikely Path to Public Trust Provides Lessons for the US, Brookings Institution, 2020.

Dawson, A., Innes, M. How Russia's Internet Research Agency Built Its Disinformation Campaign, The Political Quarterly, Vol. 90, No. 2, 2019.

Defending Democracy Against Authoritarian Expansion, IORG, 2021.

DFRLab, #TrollTracker: Twitter Troll Farm Archives; Part Three — Assessing an covert Iranian social media influence campaign, 2018.

Diresta, R., Grossman, S., 'Potemkin Pages & Personas: Assessing GRU Online Operations, 2014-2019', Cyber Policy Center, 2019.

DiResta, R., Goldstein, J., Grossman, S., Middle East Influence Operations: Observations Across Social Media Takedowns, Project on Middle East Political Science, 2021.

Dixon, T. and Juan-Torres, M., Is the Internet Eroding Europe's Middle Ground?, European Strategy and Policy Analysis System, 2018.

Elswah, M., Howard, P.N., "Anything that Causes Chaos": The Organizational Behavior of Russia Today (RT), Journal of Communication, Volume 70, Issue 5, October, 2020.

Emmott, R., de Carbonnel, A. and Humphries, C., Who Burned Notre Dame? Brussels Goes After Fake News as EU Election Nears, Reuters, 2019.

EU Disinfo Lab, How the Digital Services Act (DSA) Can Tackle Disinformation, 2021.

European Commission and HRVP, Action Plan against Disinformation, JOIN(2018) 36 final of 5 December 2018.

European Commission and HRVP, Tackling COVID-19 Disinformation - Getting the Facts Right, JOIN(2020) 8 final of 10 June 2020.

European Commission, Assessment of the Code of Practice on Disinformation - Achievements and Areas for Further Improvement, SWD(2020) 180 final of 10 September 2020.

European Commission, Code of Practice on Disinformation, 2021.

European Commission, Commission Presents Guidance to Strengthen the Code of Practice on Disinformation, 2021.

European Commission, Countering Illegal Hate Speech Online. 5th Evaluation of the Code of Conduct, 2020.

European Commission, European Digital Media Observatory (EDMO), 2021.

European Commission, On the European Democracy Action Plan, COM(2020) 790 final of 3 December 2020.

European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final of 15 December 2020.

European Commission, Tackling Online Disinformation, 2021.

European Commission, The EU Code of Conduct on Countering Illegal Hate Speech Online, 2016.

European Court of Auditors, Disinformation Affecting the EU: Tackled but Not Tamed, 2021.

European Digital Media Observatory, EDMO at a Glance, 2021.

Tabula.ge, European Georgia Presents Legislative Package Aimed at Mitigating Russian Propaganda, 2019.

European Parliament, European Parliament Recommendation of 13 March 2019 to the Council and the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy Concerning Taking Stock of the Follow-Up Taken by the EEAS Two Years after the EP Report on EU Strategic Communication to Counteract Propaganda against It by Third Parties (2018/2115(INI)).

European Parliament, P9_TA(2020)0009 Annual Report on the Implementation of the Common Security and Defence Policy. European Parliament Resolution of 15 January 2020 on the Implementation of the Common Security and Defence Policy – Annual Report (2019/2135(INI)).

European University Institute, National EDMO Hubs Announced, 2021.

EUvsDisinfo, DISINFO: Suspicious American Military Activity in Lugar Lab, 2020.

EUvsDisinfo, DISINFO: US Prepares Biological Weapons Against Russia, 2019.

EUvsDisinfo, Disinformation Can do Anything: From Insulting People to Ruining Them, 2021.

EUvsDisinfo, Pro-Kremlin Outlets as Amplifiers of Hate Speech in Georgia, 2021.

FactCheck.ge, About us, 2021.

Filipova, R., Galev, T., Russian Influence in the Media Sectors of the Black Sea Countries. Tools, Narratives and Policy Options for Building Resilience, Centre for the study of Democracy, 2018. See also another recent study by CSD.

Filipova, R., Stefanov, R., Countering Kremlin's Media Influence in Europe, Patterns of Anti-Democratic Messaging, Disinformation Responses, and Resilience Assets, Centre for the Study of Democracy, 2021.

Filipova, R., Vladimirov, M., Gerganov, A., Tackling Kremlin's Media Capture in Southeast Europe. Shared patters, specific vulnerabilities and responses to Russian disinformation, Centre for the Study of Democracy, 2021.

FireEye, Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East, 2018.

Fisher, M., Disinformation for Hire, a Shadow Industry, Is Quietly Booming, New York Times, 2021.

Foreign & Commonwealth Office, UK Condemns Russia's GRU over Georgia Cyber-Attacks, 2020.

Fotyga, A., Priority Question for Written Answer P-002103/2020 to the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy, 2020.

François, C., Actors, Behaviors, Content: A Disinformation ABC Highlighting Three Vectors of Viral Deception to Guide Industry & Regulatory Responses, Transatlantic Working Group, 2019.

Gelava, S. and Buziashvili, E., Online Calls for Attacks Against Georgia's LGBTQ Community Result in Offline Violence, 2021.

Georgia's Reforms Associates (GRASS), Research, 2021.

Georgia's Reforms Associates (GRASS), Statement on the Process of Drafting and the Final Report of the Thematic Inquiry Group on Disinformation and Propaganda of the Parliament of Georgia, 2020.

Georgian National Communications Commission (GNCC), Annual Report 2018, pp. 10-12, 2018.

Georgian National Communications Commission (GNCC), Annual Report 2020, pp. 95-108, 2020.

Gershaneck, K.K., Political Warfare. Strategies for Combating China's Plan to "Win without Fighting", Marine Corps University Press, Quantico, Virginia, 2020.

Gigitashvili, G. and Leroux, J., Facebook Removes Inauthentic Assets Connected to Georgian Far-Right Group Alt-Info, 2020.

Gigitashvili, G., Russia's 2019 Cyberattack against Georgia Was Followed by a Full-Spectrum Propaganda Effort, New Eastern Europe, 2020.

Global Influence Operations Report, Russian Media Legitimizes Baltic Fringe Disinformation Outlet, 2021.

Goldstein, J.A., Grossman, S., How disinformation evolved in 2020, 4 January, 2021.

Greene, S., Asmolov, G., Fagan, A., Fridman, O., Gjuzelov, B., Mapping Fake News and Disinformation in the Western Balkans and Identifying Ways to Effectively Counter Them, European Parliament, 2020.

Grinberg, N. et al., Fake news on Twitter during the 2016 U.S. presidential election, Science, Vol 363, Issue 6425, pp. 374-378, 2019;

Guess, A., Nagler, J., Tucker, J., Less than you think: Prevalence and predictors of fake news dissemination on Facebook, Science Advances 5, eaau4586, 2019;

Harold, S.W., Beauchamp-Mustafanga, N., Hornung, J.W., Chinese Disinformation efforts on social media, Rand Corporation, 2021.

Helmus, T.C., Kepe, M., A Compendium of Recommendations for Countering Russian and Other State-Sponsored Propaganda, Rand Corporation, 2021.

Hioe, B., Between Infodemic and Pandemic: The Paranoid Style in Taiwanese Politics, Popula, 2021.

Hsieh, M., Fast, Fair, Fun: Taiwan Digital Minister Audrey Tang On Pandemic Response, Ketagalan Media, 2021.

Huang, J., 'The China Factor in Taiwan's Media, China Perspectives [Online],' China Perspectives, 2017/3, 2017.

Hudson, M., What Is Social Media?, The Balance Small Business, 2020.

Iranwire Arabic, Learn About The Islamic Radio And Television Union, Which Washington Closed Most Of Its Media Outlets, 2021.

Jones, M.O, Disinformation super-spreaders: the weaponisation of COVID-19 fake news in the Persian Gulf and beyond, Global Discourse, vol 10, no 4, 431–437, 2020.

Jones-Jang, M., Mortensen, T., 'Does Media Literacy Help Identification of Fake News? Information Literacy Helps, but Other Literacies Don't,' American Behavioral Scientist, 2019.

Jowett, G.S., O'Donnell, V., Propaganda and Persuasion, SAGE Publications, Fourth Edition, 2018.

Juneau, T., How Iran Helped Houthis Expand Their Reach, War on the Rocks, 2021.

Kalenský, J., Freudenstein, R., The EU's Action Plan Against Disinformation: Good First Step, Now We Need a Follow-Up, disinfoportal.org, 2018.

Kalenský, J., A Change of Tactics: Blurring Disinformation's Source, disinfoportal.org, 2019.

Kalenský, J., Hitting COVID-19 Disinfo Websites where It Hurts: Their Wallets, medium.com/dfrlab, 2020.

Kalenský, J., The US Investigations Highlight Europe's Laxity on Disinformation, disinfoportal.org, 2019.

Kaul, A., Sockpuppet Accounts Impersonate India's Space Agency Chief, DFRLab, 2019.

Kerr, W., Phillips, M., Taiwan Is Beating Political Disinformation. The West Can Too., Foreign Policy, 2020.

Khalaji, M., Yemen's Zaidis: a Window for Iranian Influence, The Washington Institute for Near East Policy, 2015.

King, G., Pan, J., Roberts, M.E., 'How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument', American Political Science Review 111 (3), 2017.

Kintsurashvili, T., Pre-Election Monitoring: Anti-Western Messages, Hate Speech, Fake News, Media Development Foundation, 2021.

Lee, D., Hong Kong protests: Twitter and Facebook Remove Chinese Accounts, BBC News, 2019.

Lee, L. et al., Deafening Whispers China's Information Operation and Taiwan's 2020 Election, DoubleThink Lab, 2021.

Lee, Y. and Cheng, I., Paid 'News': China Using Taiwan Media to Win Hearts and Minds on Island – Sources, Reuters, 2019.

Legislative Yuan Passes Anti-Infiltration Bill to Strengthen Defense for Democracy and Preserve Stable and Orderly Cross-Strait Exchanges, Mainland Affairs Council, 2019.

Lejava, N., Georgia's Unfinished Search for Its Place in Europe, Carnegie Europe, Brussels, 2021.

Levitt, M., Hezbollah's Regional Activities in Support of Iran's Proxy Networks, Middle East Institute, 2021.

Lucas, E., Morris, J. and Rebegea, C., Information Bedlam: Russian and Chinese Information Operations During Covid-19, CEPA, 2021.

Martin, D.A., Shapiro, J.N., Ilhardt, J.G., Tracking Online Influence Efforts, 1 November, 2020.

Media Literacy Education Resource Network (媒體素養教育資源網), official website of the Ministry of Education of Taiwan, 2021.

Meister, S. et al., Understanding Russian Communication Strategy: Case Studies of Serbia and Estonia, 2018.

Monaco, N. et al., Detecting Digital Fingerprints: Tracing Chinese Disinformation in Taiwan, International Republican Institute & Graphika, 2020.

Myth Detector, About Myth Detector - MDF's Fact-Checking Platform, 2021.

Myth Detector, How Did Official Documents Leak and What Experiments are Georgian scientists Carrying Out on Bats?, 2020.

Myth Detector, How Were Documents about Lugar Lab Leaking from the Ministry of Health before the Cyberattack?, 2020.

Nabben, K., Hacking the pandemic: how Taiwan's digital democracy holds COVID-19 at bay, The Conversation, 2020.

Nardelli, A. and Silvermann, C., Italy's Most Popular Political Party Is Leading Europe In Fake News And Kremlin Propaganda, Buzzfeed, 2016.

National Security Bureau, Countermeasures Against Chinese Disinformation Psychological Warfare [中國假訊息心戰之因應對策], 2019.

NDI, Public Attitudes in Georgia: Results of December 2020 Telephone Survey, carried out for NDI by CRRC Georgia, 2021.

Nielsen, N. and Zalan, E., EU Says Orban's New National Poll Contains 'Fake News', EU Observer, 2020.

Nimmo, B, et al., Cross-Platform Spam Network Targeted Hong Kong Protests, Graphika, 2019.

Nimmo, B. et al, Spamouflage Breakout, Graphika, 2021.

Nimmo, B., et al, Return of the Spamouflage Dragon, Graphika, 2020.

Nimmo, B., The Breakout Scale: Measuring the impact of influence operations, Brookings Institute, 2020.

Nimmo, B., #BotSpot: Twelve Ways to Spot a Bot, DFRLab, 29 August, 2017.

Nyst, C., Monaco, N., State-sponsored Trolling, How governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns, Institute for the Future Digital Intelligence Lab, 2018.

Official Twitter account of the EU Ambassador to Georgia, Carl Hartzell, 2021.

Official Website of coalition for Euro-Atlantic Georgia, 2021.

Pamment, J., EU Code of Practice on Disinformation: Briefing Note for the New European Commission, Carnegie Endowment for International Peace, 2020.

Pamment, J., The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework, Carnegie Endowment for International Peace, 2020.

Parliament of Georgia, Nino Goguadze Introducing the Report of the Thematic Inquiry Group on Disinformation and Propaganda at the Briefing, 2020.

Plasilova, I. et al., Study for the 'Assessment of the implementation of the Code of Practice on Disinformation'. Final Report, 2020.

Polyakova, A., Fried, D., Democratic Offense Against Disinformation, CEPA, Atlantic Council, 2020.

Polyakova, A., The Kremlin's Trojan Horses 3.0, Atlantic Council, 2018.

Pomerantsev, P., Weiss, M., The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money, 2014.

Pompeo, M. R., The United States Condemns Russian Cyber Attack Against the Country of Georgia, 2021.

Prier, J. Commanding the Trend: Social Media as Information Warfare, Strategic Studies Quarterly, 11 (4), 2017.

Repucci, S. and Slipowitz, A., Democracy under Siege, Freedom House, 2021.

Rhynard-Geil, M. and Inks, L., The Weaponization of Social Media, ADAPT Peacebuilding, 2020.

Rid. T, Active Measures: The Secret History of Disinformation and Political Warfare. New York: Farrar, Straus and Giroux, 2020.

Rob, J.T., Shapiro, J.N., A Brief History of Online Influence Operations, Lawfare Blog, 28 October, 2021.

Roberts, D., China's disinformation strategy. It's dimensions and future, Atlantic Council, The Scowcroft Centre for Strategy and Security & The Digital Forensic Research Lab, 2020.

Sacks, D., 'What Xi Jinping's Major Speech Means for Taiwan,' Council on Foreign Relations, 2021.

Shao, C., Ciampaglia, G.L., Varol, O. et al., The spread of low-credibility content by social bots, Nature Communications 9, 4787, 2018;

Siegel, A., Official Foreign Influence Operations: International Broadcasters in the Arab Online Sphere, Project on Middle East Political Science, 2021.

Sirbiladze, I., Russian Disinformation Campaigns in Georgia: A Study of State and Civil Society Response, PMC Research Center, Tbilisi, 2019.

Snegovaya, M., Watanabe, K., The Kremlin's Social Media Inside the United States: A Moving Target, Free Russia Foundation, 2021.

Social Order Maintenance Act, Laws & Regulations Database, 2021.

Stanford Internet Observatory, Taiwan Election: Disinformation as a Partisan Issue, 2020.

Starbird, K., "Disinformation's spread: bots, trolls and all of us", Nature, 24 July, 2019;

Stengel, R., Information Wars: How We Lost the Global Battle Against Disinformation and What We Can Do About It, Atlantic Monthly Press, 2019.

Strong, M., Facebook Shuts Down Groups Supporting Taiwan KMT Presidential Candidate, Taiwan News, 2019.

Stubbs, J. and Bing, C., Exclusive: Iran-based political influence operation - bigger, persistent, global, Reuters, 2018.

Swanbeck, S., How to Understand Iranian Information Operations, Lawfare, 2021.

Taiwan Media Watch, Official Website, 2021.

Taiwan Shuts Down Pro-China CTi News, The News Lens, 2020.

Taiwan: the Non-Renewal of CTi News Channel's Licence Does Not Go Against Press Freedom, Reporters Without Borders, 2020.

Tennis, M., Russia Ramps up Global Elections Interference: Lessons for the United States, Centre for Strategic & International Studies, 2020.

Torfeh, M., The Role of Iran's Regional Media in its Soft War Policy, Al Jazeera Center for Studies, 2017.

Treyger, E., Cheravitch, J., Cohen, R.S. (n.d.), Russian Disinformation Efforts on Social Media, RAND Corporation, forthcoming.

Tseng, P. and Shen, P., The Chinese Infodemic in Taiwan, DoubleThink Lab, 2020.

Tsitsikashvili, M., Comparing Lessons Learned from Countering Russian Disinformation in Georgia and the Czech Republic, Kremlin Watch Program 2019, 2019.

Tsitsikashvili, M., Georgia's Strategic or Partisan Communications?, 2020.

Tu, C., Lessons from Taiwan's Experience with COVID-19, Atlantic Council, 2020.

Twitter Blog, Disclosing Networks of State-Linked Information Operations, 2021.

U.S. Department of Justice, United States Seizes Domain Names Used by Iran's Islamic Revolutionary Guard Corps, 2020.

U.S. Department of Treasury, Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections, 2021.

Vilmer, J.-B., Effective State Practices against Disinformation: Four Country Case Studies, Hybrid Center of Excellence, 2021,

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, Paris, August 2018.

Vosoughi, S., Roy, D., Aral, S., The spread of true and false news online, Science, Vol. 359, Issue 6380, pp.1146-1151, 2018.

Walsh, E., Disinformation in Taiwan: International Versus Domestic Perpetrators, V-dem, 2020.

Wang, A.HE., Lee, Mc., Wu, MH. et al., 'Influencing Overseas Chinese by Tweets: Text-Images as the Key Tactic of Chinese Propaganda,' Journal of Computational Social Science 3**,** 2020, 469–486.

Wang, T., 'Does Fake News Matter to Election Outcomes?: The Case Study of Taiwan's 2018 Local Elections,' Asian Journal for Public Opinion Research 8(2), 2021, pp. 67–104.

Wanless, A., How Europe Can Tackle Influence Operations and Disinformation, Carnegie Europe, 2021.

Wardle, C. and Derakhshan, H., INFORMATION DISRODER: Toward and interdisciplinary framework for research and policy making, Council of Europe report DGI(2017)09, 2017.

Whiskeyman, A., Berger, M., 'Axis of Disinformation: Propaganda from Iran, Russia, and China on COVID-19', The Washington Institute for New East Policy, 2021.

Williams, K. B., Bertrand, N., and Marquardt, A., New Intel Reports Indicate Fresh Efforts by Russia to Interfere in 2022 election, CNN, 2021.

Yang, G., 'Internet Activism & the Party-State in China,' Dædalus 143 (2), 2014.

Yang, S., Executives of 3 Taiwan TV Stations Named by 'Chinese Spy' Invited to NCC Meetings, Taiwan News, 2019.

PE 653.658
EP/EXPO/INGE/FWC/2019-01/LOT4/1/C/09

Print ISBN 978-92-846-8763-3 | doi: 10.2861/636283 | QA-01-21-473-EN-C
PDF ISBN 978-92-846-8762-6 | doi: 10.2861/495831 | QA-01-21-473-EN-N