

How OGP Members Can Address Foreign-Sponsored Information Manipulation¹

This policy brief is part of a series by OGP and NDI analyzing openness and oversight measures that prevent or counter covert foreign influences.

Summary and Overview

Autocratic governments are mounting a persistent, asymmetric challenge to democratic governments and institutions in the information domain. The health of the open information systems upon which democracies depend is at stake. Openness and oversight regulations and practices can help counter the use of foreign-sponsored information manipulation.

Table of Contents

What is foreign-sponsored information manipulation?	1
What are the goals and narratives?	3
What are the tactics?	4
How does foreign-sponsored information manipulation undermine democratic governance?	7
Sample actions to counter foreign-sponsored information manipulation	8

What is foreign-sponsored information manipulation?

Foreign-sponsored information manipulation entails the coordinated use of social or traditional media to influence public debate by intentionally disseminating or amplifying information that is false or misleading; engaging in deceptive practices like obscuring or misrepresenting the provenance or intent of content; and/or developing and spreading other forms of harmful content such as hate speech or incitement to violence. It can also involve intentionally suppressing information for political ends.

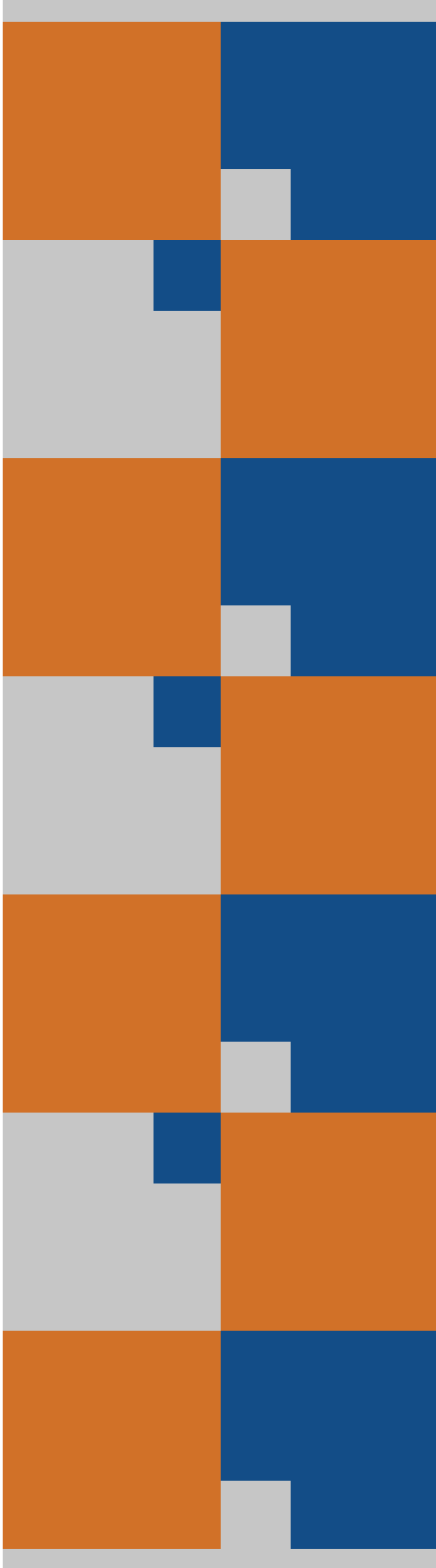
Information manipulation has become a feature of political life around the world and a threat multiplier in other domains. Information manipulation typically goes hand in hand with other means of malign influence, such as covert finance or political corruption; they build over time, exploit social and political fractures, prime audiences for future attacks and are mobilized at crucial moments (such as elections). They also require significant resources to detect and investigate.



No country has escaped the dangers of information manipulation: citizens across the world experience its harms on a daily basis. The opaque nature and diverse tactics make cross-country comparison difficult; however, a 2021 analysis of influence manipulation conducted on Facebook between 2017 and 2020 found that the countries most frequently targeted by foreign-sponsored influence operations were the United States, the United Kingdom, Ukraine, Libya and Sudan.² A recent global survey shows that almost 60 percent of internet users worry about misinformation.³ Unsurprisingly, citizens in countries with democratic governments express the greatest concern. Respectful of freedom of information and speech, and mindful of privacy concerns, open societies are more vulnerable to information manipulation and less prone to respond by controlling information and technologies.⁴

While domestic information manipulation is likely more common than state-backed influence efforts, the number and reach of governments carrying out covert operations in other countries is not insignificant.⁵ In 2020, a group of researchers identified at least seven countries using information manipulation to influence views outside their borders.⁶

It is important to note that state actors are not the sole perpetrators of foreign information manipulation. Authoritarian regimes often rely on private businesses specialized in the sale of digital manipulation.⁷ Driven primarily by profit, these private actors may not have the same goals as state actors, but their information manipulation campaigns contribute to the erosion of trust in news and the weakening of genuine democratic discourse. In a number of contexts, foreign information operations have also merged with domestic ones, whereby a variety of actors pursue similar tactics, often through collaboration. Social media companies have identified covert information manipulation networks affiliated with political parties, social movements and religious organizations.⁸



What are the goals and narratives?

Authoritarian governments engage in information manipulation to further their geopolitical goals by shifting global opinion, sowing discord and conflict and weakening trust in democracy.

A common narrative of these operations is that democratic governments are weak and ineffective. In order to draw a false equivalence with their own illiberal systems, autocratic governments use “whataboutism” — the practice of responding to an accusation with a counter-accusation or by raising a different issue — to paint democratic governments as hypocritical, in particular on issues of race in the case of the United States.⁹ During the COVID-19 pandemic, as vaccines were first rolled out around the world, illiberal influencers sought to undermine the safety and efficacy records of certain Western vaccines in order to boost skepticism of them and undermine their appeal.¹⁰ In 2021, both Russia and China were sophisticated in tailoring their messaging on vaccines to target audiences in the global south. Chinese state media highlighted the challenges of cold chain storage in hot countries and questioned pharmaceutical manufacturers’ motives in places with a history of anti-capitalism.¹¹ Beijing also positioned its own vaccines as readily accessible global public goods available to developing countries at a time when it was underperforming in delivering them. Throughout 2020, both countries also highlighted scenes of election chaos in the United States. The goal of these efforts is to diminish the appeal of democratic systems, undermine their institutions and breed mistrust in their model.



What are the tactics?

Authoritarian actors conduct covert information operations through a wide variety of tactics, often deploying multiple, overlapping strategies against a single target.

The most common forms of influence include the following types of channels and actors:

Investments in Vast Propaganda Apparatuses. Illiberal governments have put immense resources into state-backed media apparatuses. In 2021, Moscow increased its propaganda budget to about \$2.8 billion — a \$460 million increase from previous years.¹² Beijing, for its part, earmarked as much as \$6 billion for expanding state media globally as early as 2009.¹³ Both Russian and Chinese state media have dominated search engine results for geopolitically salient terms, given that search engines are built to prioritize the “freshest” or most recent content.¹⁴ Iran has also emerged as an actor with global ambitions and sophisticated digital propaganda, targeting at least 15 countries and reaching as far as Latin America.¹⁵

Proxy Influencers. Illiberal governments use a network of largely Western proxy influencers to boost the reach and resonance of their messages — adding a veneer of legitimacy and removing a degree of culpability.¹⁶ Illiberal actors amplify fringe websites, social media content, accounts and networks for the same purpose. The Swedish Defense Research Agency has identified numerous Russian think tanks with established ties to Western academics and fringe groups, trying to influence elite policy circles.¹⁷ Beijing has quietly built a network of social media personalities on Facebook, TikTok and Twitter, who echo the Chinese government’s perspective in posts seen by hundreds of thousands of people.¹⁸ These influencers work to paint a positive image of China, deflect criticism of its rights record and advance Beijing’s views on a broad range of political topics.

Domestic Voices. Illiberal actors coopt authentic domestic voices and institutions in order to create the impression that their information campaigns are genuine advocacy — in part to evade platform detection capabilities and in part to increase the perceived legitimacy of the content it promotes. They may also wish to exacerbate the politicization of content moderation debates.¹⁹ Moscow, for instance, accomplishes this task by hiding trolls within a target population, renting the social media accounts of local citizens or recruiting real activists to stoke protests.²⁰ Ahead of Madagascar’s 2018 presidential election, Russian agents recruited a cult leader to run for office in an attempt to split the opposition vote, paid local youth to attend rallies and hired journalists to cover those events.²¹



Retail Influence. Increasingly, Russian information manipulation efforts appear to target influencers within a society — for example, journalists and activists — rather than rely on large volumes of troll farm content.²² To do this, the Kremlin, for instance, works to gain the attention of authentic influencers on various social media platforms. In Europe, Russian actors have posed as locals, and sometimes as citizen journalists, to contact journalists and other policymakers, for example, and used these accounts to create and manage groups and pages and to post and comment on content.²³ They have then used different assets to amplify posts to specific audiences across various platforms.²⁴

Trolls. Saudi Arabia has developed a vast network of trolls in order to promote the regime’s image and further the government’s strategic goals domestically and internationally.²⁵ The Saudi regime created thousands of fake accounts when it severed ties with Qatar in 2017, using them to depict popular discontent within the country.²⁶ Foreign-sponsored operations may also include co-located trolls within the target population. After sinking a South Korean ship in 2010, North Korean operatives used South Koreans’ Resident Registration Numbers to create fake accounts and post messages aimed at undermining Seoul’s credibility.²⁷

Conspiracy Theories. Information operations often promote conspiracy theories to call into question official versions of political events or to advance the idea that the truth is unknowable. One recent example is the false narrative, promoted by the Kremlin, that Ukraine is developing biological weapons capabilities with the support of the Pentagon. Moscow promoted this narrative, which was picked up on multiple popular podcasts in the United States, because it serves to justify Russia’s invasion of Ukraine.²⁸

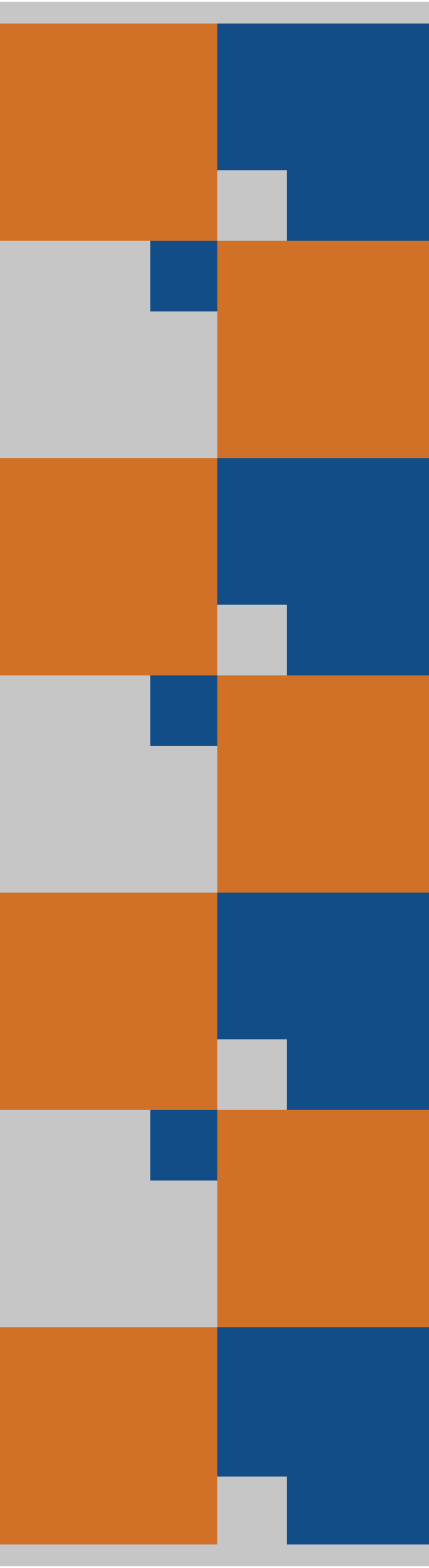
Malinformation. Illiberal states spread content that is technically true but presented in a way that is highly misleading in order to manipulate public perceptions of geopolitical issues. For example, in 2021, Russia, China and Iran regularly sensationalized reports of safety concerns around certain Western vaccines and downplayed mitigating context.²⁹ These tactics can be just as damaging as outright disinformation, but far more difficult to fact-check or otherwise respond to.



Perception Hacking. Perception hacking is an effort to create the impression of a successful operation, whether or not one has occurred. Information operators appear to recognize that they do not need to perpetuate manipulation at scale to create the impression that it did — particularly to sow doubt about an election result. Moscow has worked to leverage widespread anticipation that election interference could occur to claim that it did, even in the absence of a successful operation.³⁰ For example, ahead of the 2018 U.S. midterm elections, a website claiming to be a part of Russia’s infamous Internet Research Agency tried to spread fear of election meddling by claiming the existence of a vast operation that did not exist.

Flooding Critical Conversations. Where some state-backed manipulation focuses on denting the appeal of democratic states and institutions, others attempt to soften the images of their own illiberal regimes and dampen criticism of their human rights records. Both Saudi Arabia and China use a variety of tactics to flood conversations on their human rights record with positive content.³¹ These include hashtag campaigns and dedicated social media accounts to drown out reproval for its repressive policies.

Censorship and Repression. Illiberal governments also carry out aggressive campaigns of censorship and repression at home and surveil and work to disrupt exiles abroad, to forestall criticisms of their rights records.³² Iran practices censorship and state intimidation, including the creation of repressive cyber-police units and harassment of users, particularly women, for behaving in ways that are perceived by the regime as “un-Islamic.”³³ The Belorussian regime has shut down independent media outlets, jailed reporters, shut down the internet, blocked external platforms and banned live on-the-scene reporting at key events.³⁴



How does foreign-sponsored information manipulation undermine democratic governance?

Information manipulation by foreign, autocratic actors can undermine democratic governance through multiple pathways.³⁵ First, it often aims to drive up political polarization, which makes it hard for democratic societies to govern themselves.³⁶ Polarization, and the paralysis that often results from it, can make democratic governance seem ineffective and unappealing in contrast to authoritarian alternatives.

Second, information manipulation by foreign, autocratic actors often aims to increase skepticism about the existence of objective truth. This strikes at the very core of a functioning democracy, which depends on the idea that the truth is knowable, and citizens can discern it to make decisions of self-government. Authoritarians have no such need for a healthy information space to survive, which affords them a degree of immunity: they can pollute the information space without much concern for the global information commons.³⁷

Third, information manipulation by foreign, autocratic actors frequently seeks to depress trust in democratic institutions — including democratic governments, but also authoritative, independent media; multilateral organizations; and even the open web.³⁸ This too can expose domestic fissures, weakening democratic societies from within by distracting and dividing them.

Fourth, authoritarian actors may carry out information manipulation in support of a preferred political candidate or party. Efforts to tilt the electoral playing field influence the exercise of public authority in ways that favor the perpetrating government over the public interest. Information manipulation aimed at influencing elections and policy debates subverts a voter's right "to form opinions independently, free of violence or threat of violence, compulsion, inducement or manipulative interference of any kind."³⁹

Political leaders within open societies, and especially democratic reformers, are frequently the target of multiple, long-running campaigns to denigrate them or make them appear weak and ineffective. Research indicates that illiberal leaders disproportionately target women politicians and activists.⁴⁰



Sample actions to counter foreign-sponsored information manipulation

The following are examples of the types of commitments that OGP members can take to counter information manipulation. Though they were developed with foreign-sponsored threats in mind, many of the measures are also relevant for countering domestic-sponsored information manipulation.

Facilitating knowledge-sharing across government

Governments can play a critical role in creating new bodies or strengthening existing ones, and in supporting cross-government actions to better understand foreign information manipulation within their borders and beyond.

- ◆ **Creating an information integrity advisory committee:**
Policymakers may task a specific unit to convene an advisory committee that can identify and address trends in the information space across government functions. These bodies should include civil society and industry representatives and be empowered to function in an advisory capacity only. Their focus should be on the activity of foreign states, not domestic actors.
- ◆ **Creating interagency or interministerial working groups:**
The executive can help decision-makers across government develop a nuanced understanding of the complex causes and consequences of foreign-sponsored information manipulation through the creation of working groups. By linking different agencies or ministries that normally work in silos, the executive office can better generate a coordinated threat picture, recognizing that information manipulation is only one tool of foreign interference often used in conjunction with others, particularly cyber operations. This can be added to the mandate of an already existing body, if appropriate, or may be part of a new body.
 - ▮ To ensure working groups are not carrying out this mandate in a vacuum, it would be helpful for a country to heighten its participation in multi-stakeholder processes and other international bodies that work on freedom of expression, privacy and technology issues. For a list of relevant bodies, please see the International and Multi-Stakeholder Processes bullet point in the “Recommendations for non-government actors” below.

- 
- ◆ **Creating an ad hoc parliamentary investigative commission:** Legislators can create a specific committee to understand the complex legal, technical and political issues involved in foreign information manipulation threats, as well as to raise public awareness and generate recommendations. In 2018-19, the UK parliament’s Digital, Culture, Media and Sport Committee conducted an 18-month inquiry on the disinformation caused by ‘malign forces’ that covered individuals’ rights over their privacy, how their political choices might be affected and influenced by online information, and interference in political elections both in the UK and across the world.⁴¹

Regulating social media platforms

To increase the transparency and public accountability of social media platforms, governments can pass legislation that defines harmful content, establishes when and how such content should be removed, and levies fines against companies that do not follow the rules. In applying such measures, **it is essential that governments abide by international human rights standards stipulating that any restriction to the right of free expression be provided by law and strictly necessary for respect of the rights or reputations of others; and/or for the protection of national security or of public order, or public health and morals.**⁴²

These restrictions should also be non-discriminatory, time-bound and subject to oversight by national or international bodies.⁴³

Safeguarding Democratic Freedoms: *The measures included in this brief represent a menu of options for OGP members. Any measure under consideration should take into account the political culture and implications for freedom of expression, privacy and other citizen rights. It is particularly important to ensure that the remedy is proportional to the problem and to abstain from responses that might be manipulated, for instance, by criminalizing speech threatening the ruling party or the armed forces. National legislatures should ensure there is a legal avenue for CSOs and individuals affected by the measures to challenge anti-propaganda laws or any measure that potentially restricts freedom of expression.*

To deter or address inappropriate government takedown of content or accounts, regulatory agencies can create, disseminate and uphold standards related to takedowns of content or accounts, and audit the process by which governments request such actions. Legislators can also mandate the disclosure of government requests sent to social media and traditional media outlets to take action to remove specific content or accounts. Details on social media takedown reporting can be found in the “Recommendations for non-government actors” section below.



- ◆ **Passing legislation to regulate social media platforms:**


Legislators can introduce policies to counter disinformation and the misuse (such as false flag operations, political manipulation and online violence) of social media platforms. There are numerous examples that can serve as lessons for future legislation or their amendments. These include Germany’s Network Enforcement Act (NetzDG); the EU’s General Data Protection Regulation, Digital Markets and Digital Services Act Package; and Australia’s Sharing of Abhorrent Violent Material Act.⁴⁴ Following are examples of some policy measures:

 - ▶ Legislation may require social media companies to regularly report information about content moderation decisions in order to generate accountability through transparency, while incentivizing responsible behavior on the part of companies. Reporting requirements can contribute to building resilience to foreign information manipulation by improving the collective understanding of how platforms function (and therefore what opportunities exist for manipulation by foreign actors), as well as what types of content moderation measures they enact to defend against foreign disinformation and other harmful campaigns.
 - ▶ Legislation can also create incentives for companies to responsibly balance equities in content moderation decisions and equip lawmakers and the public to hold platforms accountable for failures to responsibly defend against foreign information manipulation, including in non-Western contexts.
 - ▶ Legislators can also require reporting on advertisements, particularly political advertising and algorithms, or the technical systems that moderate content.
 - ▶ Subnational policymakers can also pass impactful regulations, especially when representing important provinces or states. Though such federal or national legislation is missing in the United States, state-level legislation passed by California and Illinois also provides potential models to address information manipulation, including by foreign actors.



Beware of Copycat Laws: Democratic governments should be mindful that regulations adopted at home can be used to justify policies that infringe upon digital rights elsewhere. Take, for example, NetzDG, a German law that obligates social media platforms with over two million users to remove “clearly illegal” content within 24 hours and all illegal content within seven days of it being posted or face large fines. It not only created incentives for platforms to err on the side of taking borderline content down, but it also triggered a proliferation of copycat laws in countries that are considerably less free. According to one study, within just a few months, at least 13 countries adopted or proposed models similar to NetzDG.⁴⁵ Five of those countries were ranked “not free,” and five were ranked “partly free” by Freedom House that year. This risk should not forestall democratic governments from enacting regulation entirely – but it means they need to be thoughtful in their approaches and plan ahead to ensure they do not inadvertently give autocrats a talking point or blueprint to target dissent or pluralism. Many cases examined in the CEPPS Countering Disinformation Guide on legal and regulatory approaches show how such laws can be abused, but also offer potential alternatives for regulating platform; for instance, to provide election information or to regulate campaign advertising and posting.⁴⁶

- ◆ **Strengthen existing oversight bodies and functions to monitor information manipulation trends and platform abuses:** Strengthening oversight could focus on ensuring greater independence of audiovisual oversight bodies, as well as building the expertise necessary to track and expose information manipulation and make policy recommendations. In some countries, these may be government bodies (such as data protection authorities), multistakeholder advisory bodies or private-sector convened oversight bodies. In the United Kingdom, the mandate of the communications regulator, Ofcom, was expanded to include monitoring of online harms as well. Some countries lack regulatory agencies or independent bodies with the specific expertise needed to tackle the complexity of domestic and foreign information manipulation. In these cases, it may be necessary to create a new expert oversight agency to fill this gap. For a state-level example, California created a Privacy Protection Agency in 2020, while Australia created a national eSafety Commissioner in 2015. In many cases, these bodies are able to make references to judicial and human rights bodies who are better able to balance the protection of information integrity with other rights such as free speech.

- 
- ◆ **Strengthening judicial or quasi-judicial oversight of platform violations:** If an expert agency is not given the power to resolve disputes related to platform violations, legislation may create a pathway for judicial enforcement of legislation related to social media content in the context of other rights including free expression, privacy and free assembly. In keeping with the principles of open government, such tribunals should allow the public to observe and register complaints.

Standards and Guidance: Existing legislation and standards on information manipulation

To facilitate third-party auditing of content moderation practices and algorithmic systems that curate information by independent researchers, lawmakers could work to advance measures that would improve platform transparency. A transparency reform that could serve as a useful model is the European Union’s landmark Digital Services Act (DSA), which would require social media platforms to, among other things, disclose how their services amplify divisive content.⁴⁷ It would also require them to stop targeting online ads based on a person’s ethnicity, religion or sexual orientation, which could result in greater transparency to the extent that it prevents messages from reaching narrow audiences without scrutiny by a wider public. And it would require so-called very large service providers to conduct annual audits of systemic risks posed by their businesses.

Going forward, lawmakers around the world could conduct a dialogue with European counterparts on approaches to improving platform transparency for the purpose of drawing lessons from their recent experience advancing regulatory frameworks. Recognizing that this piece of legislation will have a global effect, policymakers in the global south could consider establishing means of exchange with European regulators to ensure their perspectives are represented in the process.



Creating credibly independent media ecosystems

Legislators can create independent agencies with financial independence from the legislature to oversee state-supported media outlets such as public television or radio. This, and other measures to protect the independence of public media, are described in more detail below.

- ◆ **Banning donations of foreign propaganda:** Legislators can pass laws to create and enforce outright bans of foreign propaganda content “donations” to state-run media networks. For more details, see the box below on the links between pro-Russian propaganda networks and a public news station in the Slovak Republic.
- ◆ **Budgeting measures:** Introducing legislation to “ring-fence” budgets (in this case, where the revenues, costs and financial accounts for state-run media are separated from direct manipulation by the executive) can limit the ability of government officials to abuse their access to state-run media by manipulating content through financial coercion.
- ◆ **Periodic review:** Legislators can also establish a system of periodic review of state-run media channels. When not under periodic review, rules should limit interference with day-to-day operations, budgeting or programming. Rules should also ensure standards compliance with truth-in-reporting and the transparency of donations and funding sources. Examples of state-run media outlets with periodic review are the British Broadcasting Corporation in the UK and National Public Radio in the United States.
- ◆ **Public ombudsman/inspectorate oversight:** The creation of a specific ombudsman within media organizations can provide a critical oversight function that is separate from a regulatory body, by receiving and/or investigating complaints related to information manipulation. Ombudsmen can also, if mandated, identify system-wide issues in the independent media ecosystem that may encourage the spread of domestic and/or foreign information manipulation in a country.
- ◆ **Ethics and quality guidelines:** In addition to formal rules and regulations, state-owned media often establish voluntary ethical and quality standards to guide their journalism. Though largely unenforceable, these values can provide a normative benefit to state-run outlets.



Uncovering pro-Russian information manipulation in Slovak public news

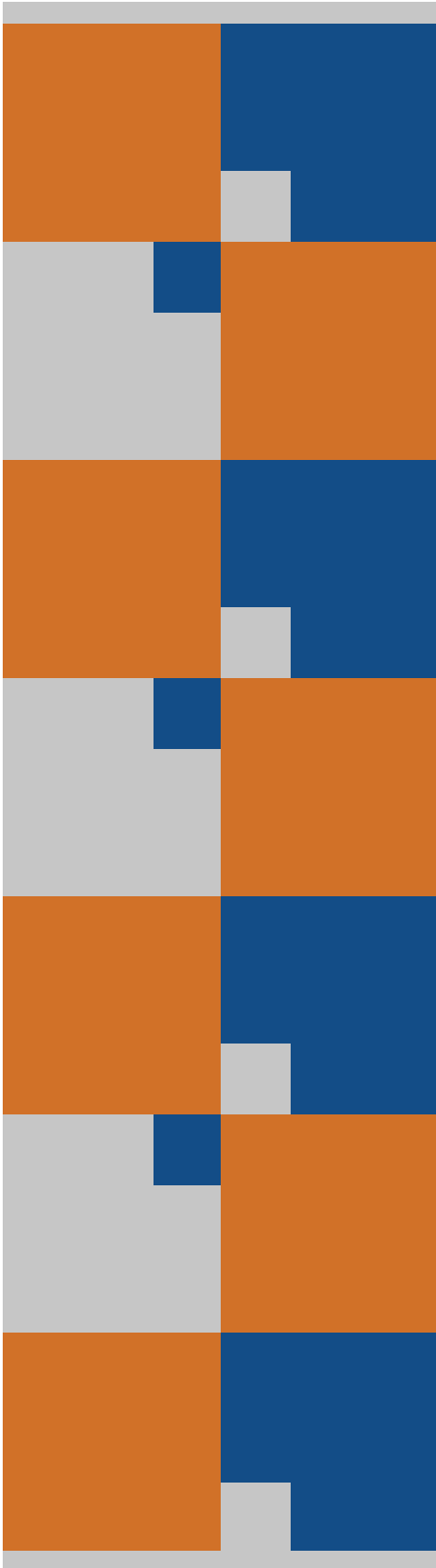
The case of the Slovak Republic illustrates how foreign information manipulation can undermine the credibility of a national media ecosystem.⁴⁸ The country's largest public news agency, TASR, has had concerning connections to Russian media sources.⁴⁹ Notably, TASR has been found to be involved in the subtle promotion of Russian information manipulation. Specifically, TASR disseminates reports from TASS, the Russian news service, often without differentiating the Russian-sourced content from its own. This is particularly problematic for local media stations relying on TASR for news — without this differentiation, local news stations inadvertently spread information manipulation from Russia. Following the Russian invasion of Ukraine, the Slovak government stepped up its efforts to combat disinformation. The government created the Center for Combating Hybrid Threats to analyze disinformation and develop strategies to address it, among other measures to create resources and legal frameworks to stop its spread.⁵⁰

Empowering civil society and the public as partners

Media outlets and civil society organizations (CSOs) can track patterns of information manipulation and identify malign actors and networks. Media and CSOs can also demand public accountability from governments and platforms. Legislators can take several actions to protect and promote non-state actors countering information manipulation.

◆ Facilitating public dialogues on problems and solutions

- ▶ **Hearings on information manipulation and countermeasures:** National legislators can create opportunities for dialogue that tap into the knowledge of media and CSOs by convening hearings to better understand the specific context in which foreign information manipulation spreads in a given country. Such hearings also provide an opportunity to co-create strategies to address information manipulation through civic participation.
- ▶ **Information-gathering meetings:** Local legislators can host town halls and other public consultation meetings with CSOs, media and other representatives of public interest (or join existing meeting spaces that CSOs already run) to understand the nature and scale of information manipulation at a more granular level, which can then be fed into state- or national-level policies.



◆ **Strengthening rights and protections for groups that counter information manipulation**

- ▶ **Facilitating civil society engagement with platforms:** Policymakers can bring together a diverse set of stakeholders and empower civil society; in particular, to contribute to the establishment of norms and commitments. In 2018 and 2022, the European Commission facilitated dialogue between civil society, social media companies and research groups to develop a Code of Practice on Disinformation.⁵¹
- ▶ **Mandating the release of media beneficial ownership data:** Legislators can mandate public disclosure of beneficial ownership and financing arrangements for all media outlets as a necessary step for building trust and protecting against capture and market concentration, which CSOs and investigative journalists can use to hold bad actors to account. Beneficial ownership policies and other legislative efforts could provide a model for this recommendation. Ideally, beneficial ownership transparency would extend to all companies, rather than the typical large companies targeted by this type of open data-driven oversight.
- ▶ **Protecting free speech, whistleblowers and the re-use of data:** Legislators can pass or strengthen protections for citizens, organizations, civil servants, private sector actors and media that face retaliation. Specific measures include limiting defamation and libel lawsuits; limiting strategic litigation against public participation (SLAPP); limiting retaliation against whistleblowers and providing incentives for exposing waste, fraud and abuse; and carrying out oversight to defend human rights advocates.
- ▶ **Protecting the right to information:** The creation or strengthening of official information acts (also known as “freedom of information” or “right to information”) to ensure public access to government information can provide an avenue of public accountability for governments that partake in information manipulation. Any exceptions to the information that can be shared publicly should be reasonable.

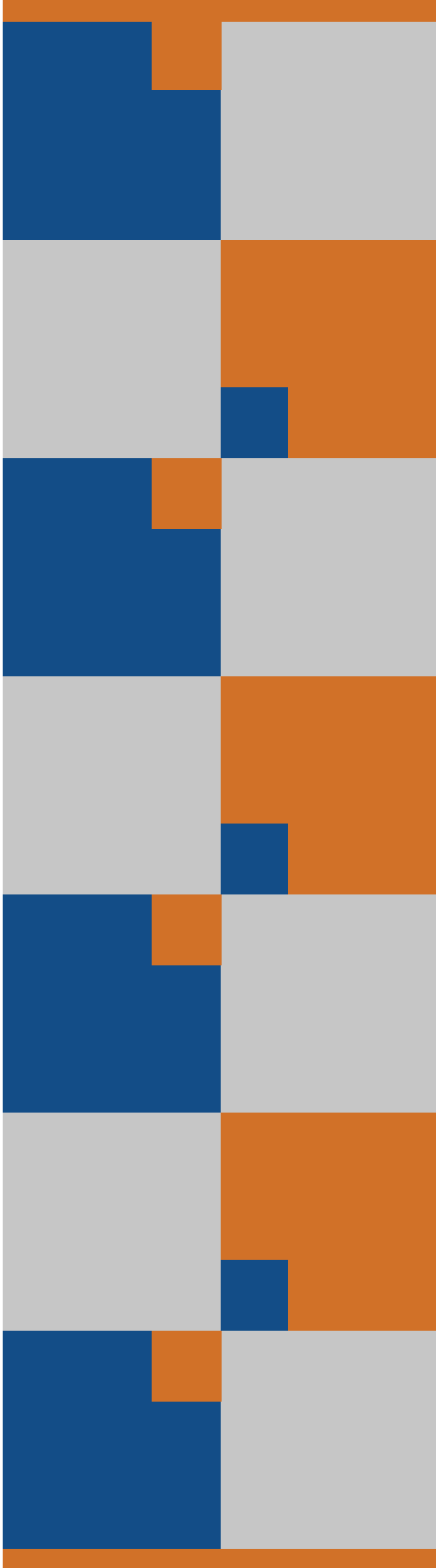


◆ **Budgeting to empower non-state partners**

- ◆ **Advancing digital literacy:** Related to funding for CSOs and media, legislators can allocate government funding for civic education and digital literacy programs that empower the public to identify disinformation and other harmful forms of content themselves. Given that influence, campaigns have shifted from public accounts to private group chats, providing the public with the tools to counter negative content, particularly in their own networks, can weaken the effect of disinformation and its damaging counterparts on public discourse. For their part, CSOs can provide fact-checking information and other resources to increase the reach of such educational initiatives, particularly by working with marginalized groups and/or in regions that governments may not be able to reach on their own.
- ◆ **Offering grants to organizations that counter information manipulation:** National and local legislators can support existing monitoring efforts by providing financial support to CSOs to carry out their work, such as through government grants.

◆ **Limiting retaliatory and anti-speech legislation:** Legislators can pass laws to limit the government’s ability to abuse defamation and libel laws, which can be used to suppress criticism of the government under the guise of stamping out “fake news.” Legislators can also provide an avenue for citizens to seek legal remedies when governments apply information manipulation measures to forward harmful interests. The following examples illustrate how the lack of safeguards can create opportunities to stifle dissent.

- ◆ As representative of a trend throughout Southeast Asia, legislators in the Philippines’ House of Representatives filed a bill to criminalize the creation and dissemination of “fake news” in early August of this year.⁵² Organizations such as Human Rights Watch have raised concerns about the lack of clarity in the bill on how the government would differentiate between false and true content.
- ◆ In 2019, the Tanzania Parliament amended its Statistics Act of 2015, perhaps in response to pressure from local and international CSOs and multilateral institutions.⁵³ The original act and its amendment in 2018 criminalized the publication of statistics without the approval of the National Bureau of Statistics.



Croatia: OGP Commitment on the Media Regulations Framework (2018)

Media freedoms in Croatia have declined in recent years, including increased political interference in the media and attacks against journalists.⁵⁴ The government controls a majority of advertising funds through publicly-controlled monopolies, and news reports accused the government of secretly controlling media coverage of the government's response to the COVID-19 outbreak.⁵⁵ There are also issues regarding journalism ethics and standards, lack of editorial accountability and increasing problems with "fake news," particularly on non-linear platforms.

Croatia committed to ensuring greater transparency and independence of the media industry in its third OGP action plan. Milestones for the commitment include drafting legislation to increase media transparency and establishing a beneficial ownership register for the media industry. The commitment also aims to combat fake news by increasing public trust in the media and improving media literacy.

Expanding data protections and oversight of data processing

Data Protection Authorities (DPAs) are independent bodies that supervise the application of data protection laws. Though originally conceived to address data violations related to state security, fraud (such as the hacking of individuals' data) and privacy, the mandate of DPAs overlaps with disinformation through the ways in which states can abuse user data for personalized manipulation, including through the microtargeting of political ads, or by hacking information to weaponize in an information op.

- ◆ **Strengthening DPAs:** Legislators should consider creating this type of body where it does not already exist or strengthening it to effectively respond to violations of data protection laws. To expand the oversight of data protections and data processing (such as automated decision-making), DPAs can provide an expert understanding of data protection issues. However, to effectively take on this oversight role, DPAs should have an expanded mandate that goes beyond providing expert advice, to evaluate whether transparency principles have been violated, and levying penalties as needed. An overview of these possible functions is below.



- ▶ **Receiving complaints and producing reports:** This function may take different forms. For example, DPAs can vary in terms of whether reporting is periodic, if it can be initiated at the request of another agency, or if the DPA itself can initiate a report. Another difference relates to the gathering of evidence. The level of documentation DPAs can obtain depends on if they have subpoena power.
- ▶ **Employing transparency tools for social media algorithms:** There are a number of emerging transparency tools used to protect human rights and prevent anti-democratic uses of algorithms.
 - ◆ **Data processing registers:** A number of countries increasingly require algorithmic processing registers. These registers require government agencies (and in many cases, private sector actors) to disclose what data is being collected and how it is being processed. Under many laws, data processing includes the transfer and re-use of data for political advertising.
 - ◆ **Impact assessment:** Private sector actors, governments and others are increasingly taking steps to ensure that data processing minimizes negative risks and effects. Currently, most of this pertains to privacy and the hacking of sensitive data. However, there is increasing interest in transparency around bias, human rights and democracy impact assessments. Governments can take steps to mandate such measures and move towards norms and standards for assessment, mitigation and consideration of alternatives. (For a more nuanced exploration of approaches and challenges to impact the assessment of automated decision-making, see the work done by the AI Now Institute and Ada Lovelace Institute.⁵⁶) Some have even proposed the introduction of a “democracy impact assessment” of algorithms, borrowing from the collective or environmental assessment of harms already adopted worldwide.⁵⁷
- ▶ **Enforcing penalties and remedies for violations:** Depending on the scope of their mandate, some DPAs can take their fact-finding powers a step further to address foreign information manipulation, especially where such manipulation may constitute fraud or violate advertising standards. DPAs may have a mandate to refer a violator of data protection laws to a law enforcement agency for prosecution, especially when civil or criminal penalties are involved. DPAs themselves with investigatory, prosecutorial or adjudicative powers may also be able to direct a platform to remove the manipulated content in order to protect the victim. Specialized training for law enforcement personnel may be necessary to ensure appropriate responses and rights protection.



Increasing election and campaign transparency

Election-related information manipulation can have far-reaching consequences, which is why this form of information operation is given special attention here. Though the recommendations below primarily concern the responsibilities of electoral management bodies (EMBs), ensuring that these measures are implemented to complement those above can increase the effectiveness of a country's countermeasures.

- ◆ **Political campaign spending transparency:** EMBs can expand transparency for political campaigning and finance to cover new funding, spending and campaigning tactics for both digital and traditional broadcast expenditures. One such spending tactic is the hiring of private “strategic communication” firms, often in other countries, to push disinformation narratives to favor a campaign.⁵⁸ This trend, according to a 2020 University of Oxford media survey, is a global issue — the research found that state actors in 56 percent of countries surveyed (46 out of 81) used these firms in political campaigns.⁵⁹
- ◆ **Online political advertising:** Legislators should develop regulations and guidelines for transparency and accountability for use of online political advertising, which EMBs can enforce. Legislators should also establish avenues for oversight agencies, such as courts and regulatory agencies, to identify and regulate what constitutes acceptable political advertisements.
 - ▶ **Political ad repositories:** Given their power to independently oversee elections, EMBs can create a universal political ad repository. As campaigns are multichannel and multiplatform, a unified repository enables a comprehensive picture and informed critical debate about the content and funding of political ads. This recommendation can also facilitate the monitoring efforts led by other media organizations and CSOs, by improving their access to information about campaigns and their advertising practices.
- ◆ **Requiring disclosure of in-kind donations of communications support services:** Policies should include clauses related to the disclosure of donations, including any in-kind “things of value,” particularly from foreign governments. For example, legislators can mandate declarations of monetary and in-kind donations (including communications support) and provide legal clarification of what “things of value” include. Any agreements with foreign governments should also be disclosed.



- ◆ **Communicating truthful electoral results:** The executive office and its appointed administrators can boost the trust in the integrity of information originating from the government through transparent and proactive communication. This is especially relevant in the context of elections, which can be supported by oversight measures from EMBs.
 - ▶ Examples include the creation of information help desks for journalists to verify election-related information, to crowd-sourced quick counts related to polling to ensure election results are not portrayed as a fraud (particularly by a losing incumbent).
- ◆ **Campaign codes of conduct:** EMBs can work with campaigns to develop and promulgate codes of conduct for online campaigning, ranging from the responsible use of big data to the treatment of deepfakes and leaked information. Though voluntary, these commitments can not only provide additional support to an existing electoral code, but also incentivize candidates and political parties to act ethically in their campaigns in cases where there is inconsistent guidance or gaps in the law.

Countering online violence against women (OVAW)⁶⁰

Whether foreign- or domestically-sponsored, OVAW poses a deepening challenge to democracy, serving as a key tool of illiberalism and anti-rights agendas across the globe. This form of online aggression is often specifically directed against women in politics, seeking to exclude them from public life simply because they are women. Technology platforms have “the most to do” in terms of implementing interventions to protect women in politics engaging on their platforms, though governments should also work to understand, raise awareness and take appropriate measures. Potential transparency and oversight measures include:

- ◆ Social media companies should measure and report on the prevalence of gendered abuse; partner with fact-checking organizations; provide research partners with sustained access to data; and conduct and share gender-focused human rights impact assessments on their platforms;
- ◆ Governments can include specific reporting mechanisms on gendered disinformation in legislation addressing social media platforms’ transparency.

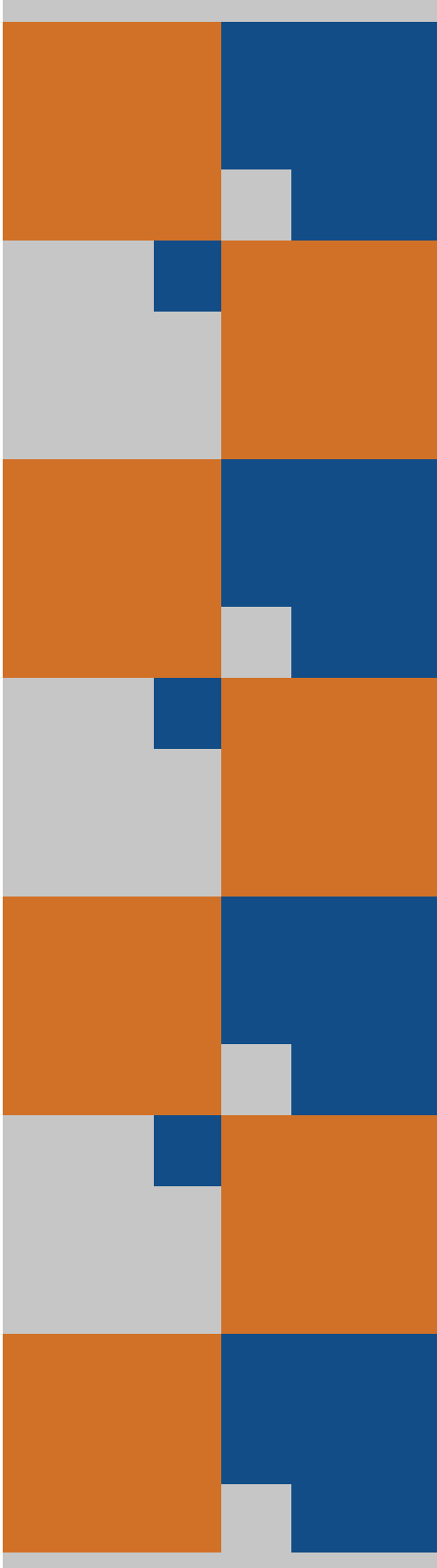


Recommendations for non-government actors

Though this paper primarily focuses on actions governments can take to diagnose, treat and prevent the spread of foreign information manipulation, the following recommendations address a few critical actions non-government stakeholders can pursue to reinforce these efforts.

International and multi-stakeholder processes: International and multi-stakeholder processes can be useful tools to support counter-disinformation strategies. A number of such initiatives are below. OGP members may choose to join or strengthen their involvement with such multilateral initiatives.

- ◆ **Santa Clara Principles:** Developed by human rights organizations, advocates and academic experts, the Santa Clara Principles support companies' efforts to comply with human rights standards. Its foundational principles include several related to transparency, with examples below.⁶¹
 - ▶ In an easily accessible location on their websites, companies should publish clear rules and policies related to when they will moderate content.
 - ▶ Users should know when a state actor has requested or participated in any action taken on their content or account.
 - ▶ Users should know when content moderation decisions have been made in whole or in part by algorithms. They should also have some understanding of the decision-making logic of automated processes related to content moderation.
- ◆ **EU Code of Practice on Disinformation:** More than 30 signatories from across different sectors (including social media platforms, advertising industry members and civil society groups) have signed to date.⁶² The code includes commitments to demonetize disinformation; support information and media literacy initiatives; and improve the disclosure of data for research on disinformation, among other measures. The code also establishes a Transparency Center accessible to all EU citizens, to document progress toward implementing the code's measures.
- ◆ **The Global Network Initiative (GNI) Principles:** GNI launched in 2008 as a multi-stakeholder process to develop principles technology companies can follow to ensure their decision-making respects freedom of expression and privacy rights.⁶³ Participants in GNI are technology companies, CSOs (like press freedom organizations), academics and investors. For details, see the Implementation Guidelines.⁶⁴



- ◆ **Organization for Economic Co-operation and Development (OECD) Artificial Intelligence Principles:** The governments in the OECD, along with additional adherents, have committed to promoting the development of trustworthy and innovative AI that respects human rights and democratic values.⁶⁵ The principles also provide recommendations for policymakers, such as guidance for investing in AI research and development.

Social media platforms: Social media platforms can complement regulatory processes using the following measures:

- ◆ **Monitoring and publishing progress data:** Social media platforms can use a “measurement, reporting and verification” (MRV) system to create indicators that can be measured methodically, reported publicly for regulators, researchers and the public, and verified through independent review. For example, these indicators can track platform actions related to content moderation, such as YouTube’s “Violative View Rate,” which seeks to determine what percentage of views on the platform comes from content that violates its policies, to evaluate whether changes to its content moderation algorithm are effectively preventing harmful videos from being viewed.⁶⁶ Ideally, these indicators will be designed with relevant regulatory agencies, non-governmental expert groups and other key stakeholders. Access to this information would enable independent researchers to better understand the nature of various online harms and go a long way toward building resilience within democratic societies. Robust researcher access to data can also help academics and civil society groups expose individual information campaigns, preventing their continuation and teaching defenders how to evolve and improve.
- ◆ **Takedown and appeals transparency:** As governments should provide takedown data on their requests for the sake of transparency, social media platforms should also report on the number of requests received, the number of accounts and/or content items impacted by the requests and how the platform responded. It would be helpful to disclose information related to the reach of information manipulation campaigns (including by foreign actors and networks) — though Facebook disclosed the number of accounts removed and their followers in their 2021 threat report, it did not describe the number of views the information manipulation posts received.⁶⁷
 - ▶ **Disaggregating government requests:** Separate government requests from private sector requests (such as those related to copyright claims), which currently is not the norm. For an example, see this report from Google.⁶⁸



- ▶ **Creating (or strengthening) an appeals process:** Establish clear appellate processes to ensure that takedown requests are reasonable and in line with the law and company policy. For an example of what a fair, transparent and accessible process can look like, see this open letter to Mark Zuckerberg, penned by the Santa Clara Principles advocates.⁶⁹
- ◆ **Whistleblower protection policies:** Social media platforms can adopt standards and guidance to protect company whistleblowers who report violations of the law. Creating internal channels for constructive dissent, especially around issues of disinformation and human rights violations, is critical to ensuring public accountability and transparency in company decision-making.
- ◆ **Supporting independent research:** Social media companies can support research in multiple contexts and languages. The study of information manipulation has been largely focused on the United States and Europe, even though the majority of social media platform users reside elsewhere.⁷⁰ The findings of that research may not be generalizable to other democracies. Researchers could be vetted by a third party to confirm their project, experience and background, and potentially sign agreements to ensure that they will care for the data and follow ethical best practices in its use.

How the Taiwanese government is supporting CSO fact-checking efforts

One example of an effective public-private partnership that builds upon the expertise of CSOs is the Digital Accountability project, a collaboration between Taiwan’s Legislative Yuan and third-party fact-checking organizations.⁷¹ The project provides a fact-checking service on the Line messaging app called the “Line Fact Checker,” which allows Line users to upload links or statements that can be compared automatically against content that has already been verified or escalated to manual review if needed.



Civil society organizations: CSOs can counter foreign-sponsored information manipulation in a variety of ways:

- ◆ **Identifying narratives and coordinated inauthentic behavior:** Civil society, often in collaboration with academics or research organizations, can help to unmask information operations.⁷² CSOs can conduct media monitoring to identify key narratives and detect coordinated inauthentic behavior. As women and other marginalized groups are often early targets of information operations, civic organizations that represent these interests are well-placed to identify the emergence of these tactics.⁷³
- ◆ **Carrying out public awareness/media literacy campaigns:** CSOs' connection to local communities position them to design and implement public awareness and media literacy programs.⁷⁴ Improved media and digital literacy among audiences could help to reduce susceptibilities to information manipulation over time.
- ◆ **Advocating vis-a-vis government:** Civil society advocacy can support transparency and oversight policies that serve to counter information operations. Additionally, CSOs have a crucial right to play as watchdogs and advocates to ensure that government responses to information operations do not represent undemocratic infringements on free speech or access to information.
- ◆ **Advocating vis-a-vis social media companies:** Based on their analysis of the patterns and harms of information manipulation, CSOs can advocate for platform policy changes that respond to those specific issues. Network and coalition-based approaches to advocacy, particularly internationally, can help increase leverage through collective action.

Traditional media: Through their investigative reporting, the media can play an important role in unmasking and raising awareness of information manipulation. The media should also take care to avoid amplifying information manipulation through their reporting. Information manipulation may become its own 'beat,' requiring specialized knowledge and access to experts to ensure accurate reporting. By publicly demonstrating their transparency and professionalism, the media can also help the public distinguish between legitimate journalism and information manipulation. Fact-checking, attribution, validation and contextualization are requirements of ethical journalism and critical to building public trust. Press councils or media self-regulatory organizations have an important responsibility to safeguard media integrity and quality.



Philanthropists and other private sector funders: Philanthropic actors and other private sector companies can support the work of free and independent media, as well as civil society researchers, to continue their work. Given the challenges in securing steady funding that many media organizations and CSOs face, philanthropy and/or the private sector could provide critical financial support through grant-making opportunities.

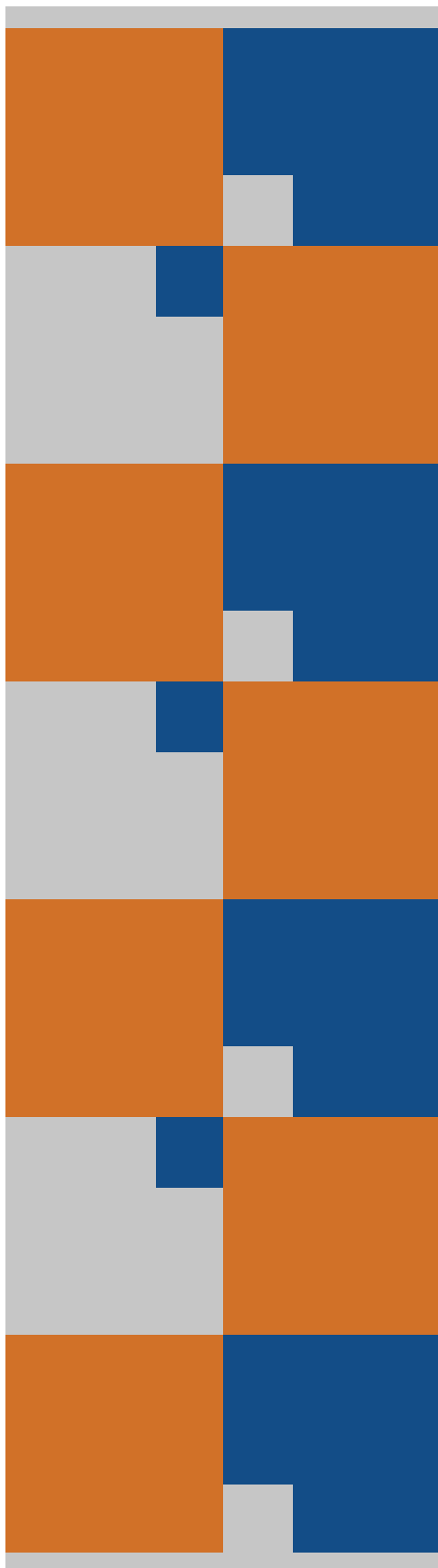


Endnotes

- 1 Contributors include Jessica Brandt, Joseph Foti, Christina Socci, Corina Rebegea and Daniel Arnaudo.
- 2 “Threat Report: Combatting Influence Operations,” Meta, May 26, 2021, <https://about.fb.com/news/2021/05/influence-operations-threat-report/>.
- 3 Aleksu Knuutila, Lisa-Maria Nedert, and Philip N. Howard, “Who Is Afraid of Fake News?” Modeling Risk Perceptions of Misinformation in 142 Countries,” *Harvard Kennedy School Misinformation Review*, April 12, 2022, <https://misinforeview.hks.harvard.edu/article/who-is-afraid-of-fake-news-modeling-risk-perceptions-of-misinformation-in-142-countries/>.
- 4 Jessica Brandt et al., *Linking Values and Strategy: How Democracies Can Offset Autocratic Advances* (Alliance for Securing Democracy, October 2020), <https://securingdemocracy.gmfus.org/wp-content/uploads/2020/10/Linking-Values-and-Strategy.pdf>.
- 5 “Domestic Disinformation on the Rise in Africa,” Africa Center for Strategic Studies, October 6, 2021, <https://africacenter.org/spotlight/domestic-disinformation-on-the-rise-in-africa/>.
- 6 Davey Alba and Adam Satariano, “At Least 70 Countries Have Had Disinformation Campaigns, Study Finds,” *The New York Times*, September 26, 2019, <https://www.nytimes.com/2019/09/26/technology/government-disinformation-cyber-troops.html>.
- 7 Hannah Bailey, Samantha Bradshaw, and Philip N. Howard, “Industrialized Disinformation, 2020 Global Inventory of Organized Social Media Manipulation,” Computational Propaganda Research Project, University of Oxford, 2020, <https://demtech.ox.ac.uk/wp-content/uploads/sites/127/2021/02/CyberTroop-Report20-Draft9.pdf>.
- 8 Josh Goldstein and Shelby Grossman, “How Disinformation Evolved in 2020,” The Brookings Institution, January 4, 2021, <https://www.brookings.edu/techstream/how-disinformation-evolved-in-2020/>.
- 9 *Dictionary.com*, s.v. “whataboutism (n),” n.d., <https://www.dictionary.com/browse/whataboutism>.
- 10 Bret Schafer et al., “Influence-enza: How Russia, China, and Iran Have Shaped and Manipulated Coronavirus Vaccine Narratives,” Alliance for Securing Democracy, March 6, 2021, <https://securingdemocracy.gmfus.org/russia-china-iran-covid-vaccine-disinformation/>.
- 11 Lin Jing (@CHINA_DIPLOMAT), “Cold truth: South Africa won’t be able to store Pfizer’s Covid vaccine. Here’s why,” Twitter, November 13, 2020, 4:34 a.m., https://twitter.com/CHINA_DIPLOMAT/status/1327183042444734465; Shen Shiwei (@shen_shiwei), “#Senetal is in talks to buy at least 200,000 doses of #COVID19 #vaccine developed by #China’s #Sinopharm,” Twitter, January 16, 2021, 12:37 a.m., https://twitter.com/shen_shiwei/status/1350316280977502208; T-House (@thouze_opinions), “#Pfizervaccine is not so much about a snap solution for the entire world,” Twitter, November 10, 2020, 1:34 a.m., https://twitter.com/thouze_opinions/status/1326050492493914112.



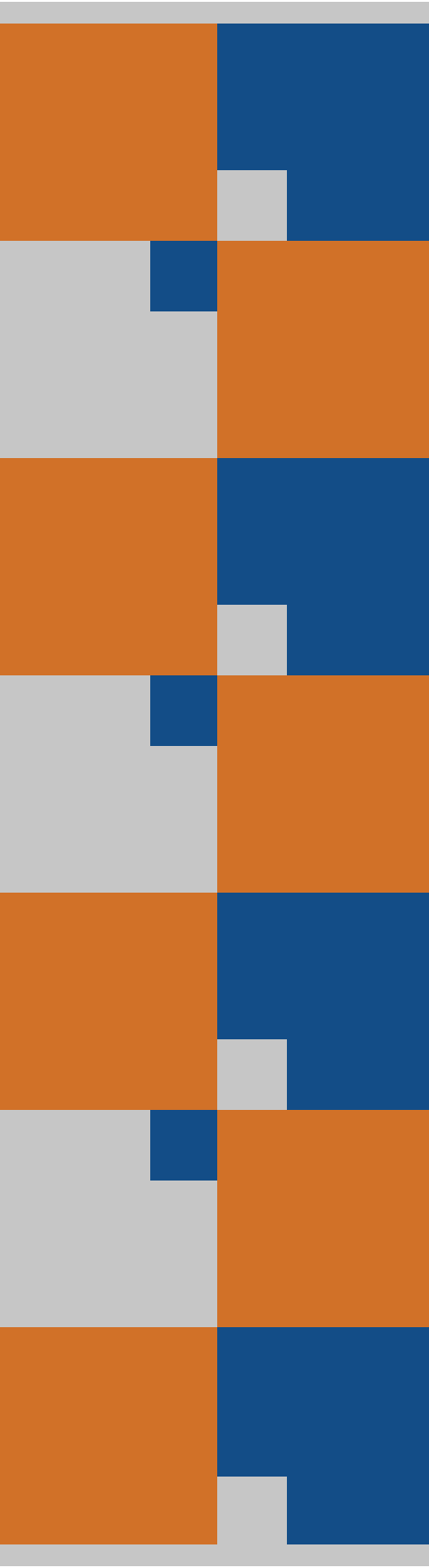
- 12 Anna Nemtsova, "Putin Ramps up RT's Propaganda Budget as Poll Ratings Slumps," *The Daily Beast*, March 5, 2021, <https://www.thedailybeast.com/putin-ramps-up-rts-propaganda-budget-as-poll-rating-slumps>.
- 13 Ibid.
- 14 Bradley Hanlon, "From Nord Stream to Novichok: Kremlin Propaganda on Google's Front Page," Alliance for Securing Democracy, June 14, 2018, <https://securingdemocracy.gmfus.org/from-nord-stream-to-novichok-kremlin-propaganda-on-googles-front-page/>; Elen Aghekyan and Bret Schafer, "Deep in the Data Void: China's COVID-19 Disinformation Dominates Search Engine Results," Alliance for Securing Democracy, October 5, 2021, <https://securingdemocracy.gmfus.org/data-void-china-covid-disinformation/>.
- 15 Emerson T. Brooking and Suzanne Kianpour, "Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century," Atlantic Council, February 11, 2020, <https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/>; Christopher Bing and Jack Stubbs, "Special Report: How Iran Spreads Disinformation Around the World," *Reuters*, November 30, 2018, <https://www.reuters.com/article/us-cyber-iran-specialreport/special-report-how-iran-spreads-disinformation-around-the-world-idUSKCN1NZ1FT>; Michael Barak and Jorge Parades Esteban, "Propaganda, Narratives and Influence in Latin America: Iran, Hezbollah and Al-Tajammu," International Institute for Counter-Terrorism (ICT), Reichman University, July 3, 2022, <https://ict.org.il/propaganda-narratives-influence-operations-latin-america/>.
- 16 Jessica Brandt and Bret Schafer, "How China's 'Wolf Warrior' Diplomats Use and Abuse Twitter," The Brookings Institution, October 28, 2020, <https://www.brookings.edu/techstream/how-chinas-wolf-warrior-diplomats-use-and-abuse-twitter/>.
- 17 Susanne Oxenstierna and Caroline Vendil Pallin, *Russian Think Tanks and Soft Power* (The Russia Programme at FOI, September 2017), <https://www.foi.se/rest-api/report/FOI-R--4451--SE>; Ibid.
- 18 Mike Catalini, Amanda Seitz, and Eric Tucker, "How China's TikTok, Facebook Influencers Push Propaganda," The Associated Press, March 30, 2022, <https://apnews.com/article/china-tiktok-facebook-influencers-propaganda-81388bca676c560e02a1b493ea9d6760>.
- 19 Jessica Brandt, "How the Kremlin Has Weaponized the Facebook Files," The Brookings Institution, November 16, 2021, <https://www.brookings.edu/techstream/how-the-kremlin-has-weaponized-the-facebook-files/>.
- 20 Gaelle Borgia and Michael Schwartz, "How Russia Meddles Abroad for Profit: Cash, Trolls and a Cult Leader," *The New York Times*, November 11, 2019, <https://www.nytimes.com/2019/11/11/world/africa/russia-madagascar-election.html>; Sheera Frenkel and Michael Schwartz, "In Ukraine, Russia Tests a New Facebook Tactic in Election Tampering," *The New York Times*, March 29, 2019, <https://seic.my.workfront.com/project/633f39b800100db291aa6c14a2db495d/documents>; Elizabeth Dwoskin, Tony Romm, and Eli Rosenberg, "The Moment When Facebook's Removal of Alleged Russian Disinformation Became a Free-Speech Issue," *The Washington Post*, August 1, 2018, <https://www.washingtonpost.com/technology/2018/08/02/moment-when-facebooks-removal-alleged-russian-disinformation-became-free-speech-issue/>.



- 21 Gaele Borgia and Michael Schwirtz, “How Russia Meddles Abroad for Profit: Cash, Trolls and a Cult Leader,” *The New York Times*, November 11, 2019, <https://www.nytimes.com/2019/11/11/world/africa/russia-madagascar-election.html>.
- 22 Jessica Brandt and Amber Frankland, “Leaks, Lies, and Altered Tape: Russia’s Maturing Information Manipulation Playbook,” Alliance for Securing Democracy, October 14, 2020, https://securingdemocracy.gmfus.org/russias-maturing-information-manipulation-playbook/#Practicing_tailored_influence.
- 23 Nathaniel Gleicher, “Removing Coordinated Inauthentic Behavior From Russia, Iran, Vietnam and Myanmar,” Meta, February 12, 2020, <https://about.fb.com/news/2020/02/removing-coordinated-inauthentic-behavior/>.
- 24 C. Shawn Eib et al., “From Russia With Blogs,” Graphika, February 2020, https://public-assets.graphika.com/reports/graphika_report_from_russia_with_blogs.pdf.
- 25 Katie Benner et al., “Saudis’ Image Makers: A Troll Army and a Twitter Insider,” *The New York Times*, October 20, 2018, <https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html>.
- 26 Marc Owen Jones, “Qatar Blockade: Saudi-Led Disinformation War Is the Tip of the Iceberg,” Middle East Eye, June 2, 2020, <https://www.middleeasteye.net/opinion/qatar-blockade-saudi-led-disinformation-war-just-tip-iceberg>.
- 27 Joe Cheravitch et al., “Combating Foreign Disinformation on Social Media,” Rand, 2021, https://www.rand.org/pubs/research_reports/RR4373z1.html.
- 28 Jessica Brandt, Adya Danaditya, and Valerie Wirtschafter, “Popular Podcasters Spread Russian Disinformation About Ukraine Biolabs,” The Brookings Institution, March 23, 2020, <https://www.brookings.edu/techstream/popular-podcasters-spread-russian-disinformation-about-ukraine-biolabs/>.
- 29 Jessica Brandt and Bret Schafer, “Using the Truth to Tell a Lie: Authoritarian COVID-19 Vaccine Mal-Information Strategies,” Power 3.0: Understanding Modern Authoritarian Influence, May 6, 2021, <https://www.power3point0.org/2021/05/06/using-the-truth-to-tell-a-lie-authoritarian-covid-19-vaccine-mal-information-strategies/>.
- 30 David E. Sanger and Nicole Perloth, “‘Perception Hacks’ and Other Potential Threats to the Election,” *The New York Times*, October 28, 2020, <https://www.nytimes.com/2020/10/28/us/politics/2020-election-hacking.html>; Ben Collins, “A Russian Troll Farm Set an Elaborate Social Media Trap for the Midterms,” NBC News, November 7, 2018, <https://www.nbcnews.com/tech/tech-news/russian-troll-farm-set-elaborate-social-media-trap-midterms-no-n933781>.
- 31 Brandtley Vickery, “Mohammed bin Salman’s ‘Army of Flies’: Saudi Arabia’s Creative Spread of Disinformation and Attack on Political Dissidence,” Democratic Erosion, November 30, 2021, <https://www.democratic-erosion.com/2021/11/30/mohammed-bin-salmans-army-of-flies-saudi-arabias-creative-spread-of-disinformation-and-attack-on-political-dissidence/>; Jessica Brandt and Bret Schafer, “How China’s ‘Wolf Warrior’ Diplomats Use and Abuse Twitter,” The Brookings Institution, October 28, 2020, <https://www.brookings.edu/techstream/how-chinas-wolf-warrior-diplomats-use-and-abuse-twitter/>; Ibid.

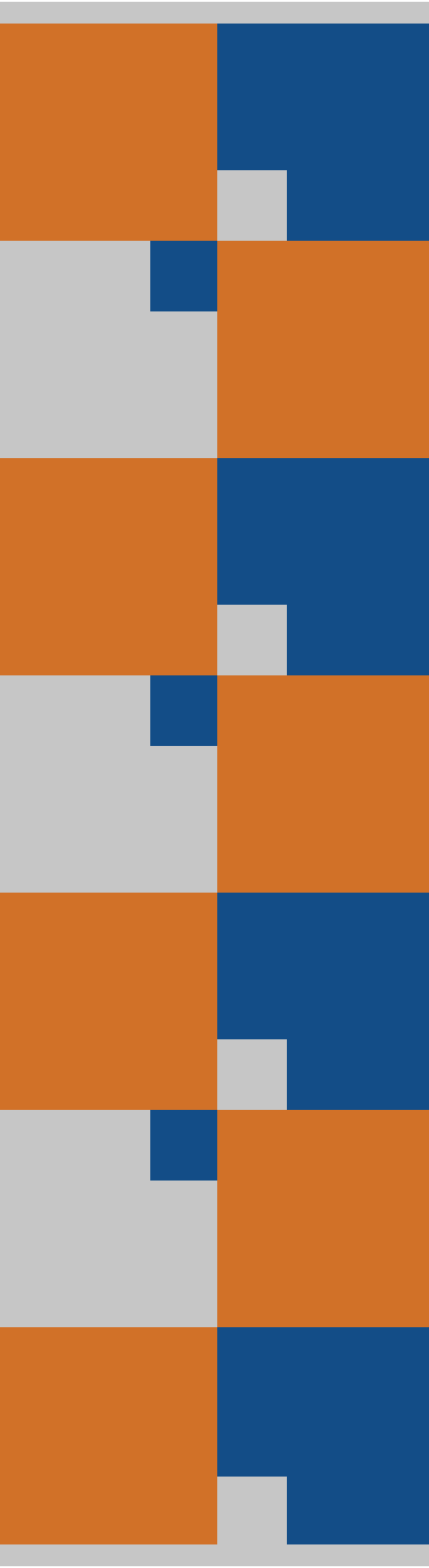


- 32 Nate Schenkkan and Isabel Linzer, *Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression* (Freedom House, February 2021), https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf.
- 33 Emerson T. Brooking and Suzanne Kianpour, *Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century* (Atlantic Council, February 11, 2020), <https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/>.
- 34 Freedom House, “Belarus: Freedom on the Net 2021,” 2021, <https://freedomhouse.org/country/belarus/freedom-net/2021>.
- 35 Daniel Arnaudo et al., *Combating Information Manipulation: A Playbook for Elections and Beyond* (National Democratic Institute, September 2021), <https://www.ndi.org/publications/combating-information-manipulation-playbook-elections-and-beyond>.
- 36 Jessica Brandt, “How Autocrats Manipulate Online Information: Putin’s and Xi’s Playbooks,” *The Washington Quarterly* 44, no. 3 (2021): 127-154, <https://www.tandfonline.com/doi/abs/10.1080/0163660X.2021.1970902?journalCode=rwaq20>.
- 37 Jessica Brandt, “How Democracies Can Win an Information Contest Without Undercutting Their Values,” Carnegie Endowment for International Peace, August 2, 2021, <https://carnegieendowment.org/2021/08/02/how-democracies-can-win-information-contest-without-undercutting-their-values-pub-85058>.
- 38 Jessica Brandt, “How the Kremlin has Weaponized the Facebook Files,” TechStream, Brookings Institute, November 16, 2021, <https://www.brookings.edu/techstream/how-the-kremlin-has-weaponized-the-facebook-files/>.
- 39 UN Committee on Human Rights, *General Comment No. 25: The Right to Participate in Public Affairs, Voting Rights and the Right to Equal Access to Public Service*, 1510th meeting, fifty-seventh session (Office of the United Nations High Commissioner for Human Rights, July 12, 1996), <https://www.equalrightstrust.org/ertdocumentbank/general%20comment%2025.pdf>.
- 40 Lucina Di Meo and Kristina Wilfore, “Gendered Disinformation Is a National Security Problem,” TechStream, Brookings Institute, March 8, 2021, <https://www.brookings.edu/techstream/gendered-disinformation-is-a-national-security-problem/>.
- 41 House of Commons Digital, Culture, Media and Sport Committee; *Disinformation and “Fake News”: Final Report* (United Kingdom Parliament, February 14, 2019), <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf>.
- 42 United Nations General Assembly, *International Covenant on Civil and Political Rights* (United Nations Office of the High Commissioner of Human Rights, December 16, 1966), <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.
- 43 “Covid-19 Triggers Wave of Free Speech Abuse,” Human Rights Watch, February 11, 2021, <https://www.hrw.org/news/2021/02/11/covid-19-triggers-wave-free-speech-abuse>.

- 
- 44 Jenny Gesley, “Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech,” Library of Congress, 2021, <https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/>; Ben Wolford, “What is GDPR?” GDPR.EU, n.d., [https://gdpr.eu/what-is-gdpr/#:~:text=The%20General%20Data%20Protection%20Regulation,to%20people%20in%20the%20EU](https://gdpr.eu/what-is-gdpr/#:~:text=The%20General%20Data%20Protection%20Regulation,to%20people%20in%20the%20EU;); European Commission Digital Strategy, “The Digital Services Act Package,” European Union, n.d., <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>; Attorney General of Australia, “Abhorrent Violent Material,” Australian Government, n.d., <https://www.ag.gov.au/crime/abhorrent-violent-material>.
- 45 Jacob Mchangama and Joelle Fiss, *The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship* (Justitia, November 2019), <http://justitia-int.org/en/the-digital-berlin-wall-how-germany-created-a-prototype-for-global-online-censorship/>.
- 46 Lisa Reppell, “Legal and Regulatory Responses to Disinformation,” Countering Disinformation, last modified April 1, 2021 <https://counteringdisinformation.org/node/2704/>.
- 47 Adam Satariano, “E.U. Takes Aim at Social Media’s Harms With Landmark New Law,” *The New York Times*, April 22, 2022, <https://www.nytimes.com/2022/04/22/technology/european-union-social-media-law.html>.
- 48 Grigorij Mesežnikov and Gabriela Pleschová, “Testing Democratic Resolve in Slovakia,” in *Sharp Power: Rising Autocratic Influence* (National Endowment for Democracy, December 5, 2017), <https://www.ned.org/wp-content/uploads/2017/12/Chapter5-Sharp-Power-Rising-Authoritarian-Influence-Slovakia.pdf>.
- 49 Ibid.
- 50 Ministry of the Interior of the Slovak Republic, <https://www.minv.gov.sk/?tlacove-spravy&sprava=ministerstvo-vnutra-aktivne-bojuje-proti-hybridnym-hrozbam-aj-na-europskej-urovni>.
- 51 European Commission Digital Safety, “Signatories of the 2022 Strengthened Code of Practice on Disinformation,” European Union, June 16, 2022, <https://digital-strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation>.
- 52 Franco Luna, “House Bill Seeks Penalties for Creating, Spreading ‘Fake News,’” PhilStar Global, August 8, 2022, <https://www.philstar.com/headlines/2022/08/08/2201195/house-bill-seeks-penalties-creating-spreading-fake-news>.
- 53 Oryem Nyeko, “Tanzania Drops Threat of Prison Over Publishing Independent Statistics,” Human Rights Watch, July 3, 2019, <https://www.hrw.org/news/2019/07/03/tanzania-drops-threat-prison-over-publishing-independent-statistics>.
- 54 “Croatia,” Reporters Without Borders, n.d., <https://rsf.org/en/country/croatia>; European Commission Staff, *2020 Rule of Law Report: Country Chapter on the Rule of Law Situation in Croatia* (European Union, September 30, 2020), https://ec.europa.eu/info/sites/default/files/hr_rol_country_chapter.pdf.



- 55 Joe Orovic, “Croatian Gov. in Secret Meeting Urged Media to Fall in Line Ahead of Coronavirus Response,” *Total Croatia News*, June 17, 2020, <https://www.total-croatia-news.com/news/44353-croatia-government-covid19>.
- 56 Dillon Reisman et al., *Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability* (Alnow, April 2018), <https://ainowinstitute.org/aiareport2018.pdf>; *Algorithmic Impact Assessment: A Case Study in Healthcare* (Ada Lovelace Institute, February 8, 2022), <https://www.adalovelaceinstitute.org/report/algorithmic-impact-assessment-case-study-healthcare/>.
- 57 Council of Europe, <https://rm.coe.int/leaflet-cahai-en-update/1680a23871>.
- 58 Max Fisher, “Disinformation for Hire, a Shadow Industry, Is Quietly Booming,” *The New York Times*, July 25, 2021, <https://www.nytimes.com/2021/07/25/world/europe/disinformation-social-media.html>.
- 59 Samantha Bradshaw, Hannah Bailey, and Philip N. Howard, *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation* (Oxford Programme on Democracy and Technology, January 13, 2021), <https://www.ox.ac.uk/news/2021-01-13-social-media-manipulation-political-actors-industrial-scale-problem-oxford-report>.
- 60 “Interventions for Ending Online Violence Against Women in Politics,” National Democratic Institute, October 2022.
- 61 Access Now et al., “The Santa Clara Principles,” Santa Clara Principles, n.d., <https://santaclaraprinciples.org>.
- 62 European Commission Digital Strategy, “The 2022 Code of Practice on Disinformation,” European Union, June 16, 2022, <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>.
- 63 “The GNI Principles,” Global Network Initiative, n.d., <https://globalnetworkinitiative.org/gni-principles/>.
- 64 “Implementation Guidelines,” Global Network Initiative, n.d., <https://globalnetworkinitiative.org/implementation-guidelines/>.
- 65 “OECD AI Principles Overview,” OECD.AI, May 2019, <https://oecd.ai/en/ai-principles>.
- 66 Jennifer O’Connor, “Building Greater Transparency and Accountability with the Violative View Rate,” YouTube Official Blog, April 6, 2021, <https://blog.youtube/inside-youtube/building-greater-transparency-and-accountability/>.
- 67 Elizabeth Dwoskin, “Facebook Reveals Broad Takedown of Global Disinformation Networks, Including Some Tied to Anti-Vaccine Groups and State Actors,” *The Washington Post*, December 1, 2021, <https://www.washingtonpost.com/technology/2021/12/01/facebook-disinformation-report/>.
- 68 “Google Transparency Report,” Google, last modified June 2, 2022, <https://transparencyreport.google.com/?hl=en>.
- 69 Access Now et al., “An Open Letter to Mark Zuckerberg,” Santa Clara Principles, n.d., <https://santaclaraprinciples.org/open-letter/>.

- 
- 70 *Social Media Platforms and the Amplification of Domestic Extremism and Other Harmful Content, Before the United States Senate Committee on Homeland Security and Governmental Affairs*, (October 26, 2021) (testimony of Professor Nathaniel Persily, James B. McClatchy Professor Law, Co-Director of the Stanford Cyber Policy Center, Stanford Law School) <https://www.dropbox.com/s/r2tgzblora0mayl/Persily%20Senate%20HSGAC%20Testimony.pdf?dl=0>.
- 71 Elizabeth Lange and Doowan Lee, “How One Social Media App Is Beating Disinformation,” *Foreign Policy*, November 23, 2020, <https://foreignpolicy.com/2020/11/23/line-taiwan-disinformation-social-media-public-private-united-states/>.
- 72 Amy Studdart, “Building Civil Society Capacity to Mitigate and Counter Disinformation: Overview – Civil Society,” *Countering Disinformation*, April 3, 2021, <https://counteringdisinformation.org/index.php/topics/csos/0-introduction-building-civil-society-capacity>.
- 73 Ibid.
- 74 Amy Studdart, “Building Civil Society Capacity to Mitigate and Counter Disinformation: Public Awareness/Media Literacy Campaigns,” *Countering Disinformation*, April 3, 2021, <https://counteringdisinformation.org/topics/csos/6-public-awarenessmedia-literacy-campaigns>.

Notes

Colophon

© 2022 National Democratic Institute and Open Government Partnership

NDI and OGP publications are independent of specific national or political interests. Views expressed in this Policy Brief do not necessarily represent the views of NDI, OGP or those of their respective Boards Members.

The electronic version of this publication is available under a Creative Commons Attribute-NonCommercial-ShareAlike 3.0 (CC BY-NC-SA 3.0) license. Portions of this work may be reproduced and/or translated for non-commercial purposes provided that NDI and OGP are acknowledged as the source of the material and are sent copies of any translation.

For more information visit the Creative Commons website: <http://creativecommons.org/licenses/by-nc-sa/3.0/>

Design and layout: Pamelyn L. Burke