

1 Introduction: Toward a comprehensive framework for countering disinformation and reinforcing information integrity

This introduction provides an overview of the challenges that mis- and disinformation pose to democracies, while flagging the need for government responses to focus on promoting integrity in the information ecosystem rather than on content. It lays out a policy framework for promoting transparent, accountable, and plural sources of information; strengthening societal resilience and relying on all actors of society; and upgrading governance measures and institutional architecture to respond to the need to reinforce information integrity.

1.1. A NEW AND RAPIDLY CHANGING INFORMATION ENVIRONMENT

Democracy depends on the free flow of information, which empowers the public to make meaningful choices, hold leaders to account, and participate actively in civic life. Access to diverse sources of information, multiple and independent news sources, and free and open discourse are all needed to enable informed democratic debate. The spread of false and misleading information, often deliberately disseminated by both foreign and domestic actors, creates confusion and polarises public debate, sowing mistrust and undermining democratic processes.

It is now well researched that the rapid and global spread of mis- and disinformation presents a fundamental risk to the free and fact-based exchange of information underpinning democratic debate (OECD, 2022^[1]).¹ While “misinformation” can be defined as false or inaccurate information that is shared unknowingly and is not disseminated with the intention of deceiving the public and “malinformation” can be described as accurate information shared to cause harm, for example by moving information from the private to the public sphere, “disinformation” is usually defined as false, inaccurate, or misleading information deliberately created, presented and disseminated to harm a person, social group, organisation or country (U.S. Department of State, 2023^[2]) (Wardle and Derakshan, 2017^[3]); (Leshner, Pawelec and Desai, 2022^[4]). Waves of false and misleading content can undermine societal cohesion, cast doubt on factual information, and undermine trust in public institutions (OECD, 2021^[5]).

Mis- and disinformation are not a new phenomenon. Propaganda, lies, and information distortions have existed – and will continue to exist – in all societies, regardless of the strength of their democracies or media environments. Likewise, individuals will continue to demand, interpret, search for, and favour information that supports their views and attitudes, particularly related to issues that are highly emotive, which can help spread misleading and false content (Westerwick, Johnson and Knobloch-Westerwick, 2017^[6]; Gupta, Parra and Dennehy, 2021^[7]; Zhao, Fu and Chen, 2020^[8]).

Advancements in digital technologies and novel forms of communication have, however, reshaped the way information is produced, shared, and consumed, locally and globally. New generative AI tools have more

recently greatly reduced the barriers to creating and spreading compelling content, while making it increasingly difficult to distinguish between what is authentic and what is manipulated. This global reach and unprecedented ability to create and disseminate content brings the challenge of mis- and disinformation into greater focus, with potentially significant impacts on social cohesion.

Deliberately false and misleading information also poses real challenges to policy implementation, with recent serious consequences in the fields of healthcare, defence and national security issues, as well as climate policies. In this context, governments are increasingly recognising their responsibility to promote information integrity – in this case, defined as information environments that are conducive to the availability of accurate, evidence-based, and plural information sources and that enable individuals to be exposed to a variety of ideas, make informed choices, and better exercise their rights. While this definition aligns with others, including, notably, the definition of information integrity in the Global Declaration on Information Integrity Online (Government of the Netherlands, 2023^[9]), the relatively recent focus on information integrity in the modern communication landscape suggests an opportunity to continue to develop this concept moving forward. More uniform understanding of what information integrity means may also facilitate measurement and evidence-based policy development.

To advance this area of work, OECD countries in the Ministerial Declaration on Building Trust and Reinforcing Democracy committed to addressing mis- and disinformation while protecting freedom of speech. Notably, the Declaration also called for strengthening representation, participation and openness in public life, embracing the global responsibilities of governments and building resilience to foreign influence, gearing up government to deliver on climate and other environmental challenges, and transforming public governance for digital democracy (OECD, 2022^[10]).

Additionally, 52 countries (of which 30 are OECD members) have come together under the International Partnership on Information and Democracy. The Partnership is an intergovernmental non-binding agreement endorsed to-date by 52 countries to promote and implement democratic principles in the global information and communication space. It was formally signed during the 74th UN General Assembly

in September 2019. In September 2023, the Governments of Canada and the Netherlands launched the Global Declaration on Information Integrity Online. Signed by 34 countries, the Declaration lays out international commitments by states to protect and promote information integrity online.

There is a growing recognition of the positive but not intrusive role governments can play in strengthening information integrity, in addition to mitigating the real threat posed by disinformation. At the same time, governments find themselves in a complex position. While action is required to counteract disinformation threats and build information integrity, this action must not lead to greater information control. Democratic governments are increasingly recognising the positive role they can – and should – play in helping promote information integrity essential to democratic discourse. The rapid and the global nature of the way information is shared now highlights that governments need to focus on comprehensive and constructive solutions by:

- Understanding how the evolution in how people get and share information affects the larger effort to reinforce democracy,
- Focusing on creating the conditions to promote information integrity, and
- Developing a framework to build information integrity, including on media and online platforms, building resilience across society, and putting in place the appropriate governance architecture.

1.2. CHANGES IN INFORMATION SPACES AFFECT DEMOCRATIC ENGAGEMENT

Advancements in digital technologies and novel forms of communication have fundamentally reshaped the way information is produced, shared, and consumed. Traditionally, media outlets were the primary channels that provided information to individuals and, as such, participated in helping them make sense of their environment, as well as forming their opinions, attitudes, and behaviour. Although always with a governance that was by nature imperfect and needed constant self-improvements, professional reporters and editors were the main information gatekeepers, guided by long-standing governance arrangements and by continually updated codes of ethics that guided their

professions, enabling media independence and diversity. Today, they no longer play as pivotal a role (Southwell, Thorson and Sheble, 2018^[11]). Anyone with an internet connection can be a content producer and distributor with massive reach, without any responsibility to adhere to information ethics and standards. In addition, the legal accountability of social media, where a significant part of this content is spread, is complex to design and enforce.

These technological advances have shifted communication and distribution approaches from “one-to-many” (typical of traditional mass media such as newspapers, radio, and television), to “many-to-many” (on online platforms) (Jensen and Helles, 2017^[12]). In addition, changing demographics are having an impact on news consumption behaviour, with younger audiences relying more on online platforms as their main sources of news. Indeed, younger generations are gravitating toward influencers and journalists that publish their content directly on social media platforms to get information (Reuters Institute for the Study of Journalism, 2022^[13]). They also increasingly want to be creators of content, which has many upsides but requires societies to rethink their information ecosystems.

While the increased accessibility and digitalisation of content provides unprecedented access to knowledge and can foster more inclusive public participation, create alternative sources of information, as well as help facilitate the creation of innovative news and media models, it has also become fertile ground for the rapid spread of false and misleading information. False information has always existed and will continue to do so; the scale, speed, and low barriers to entry offered by new communications technologies, as well as the technologies’ constant evolution, have largely driven recent changes.

Upheavals in the technologies and markets that shape information flows have also forced professional media outlets and journalists alike to increasingly compete for attention with content creators and influencers on social media platforms and have hollowed out markets for many traditional news providers, particularly at the local level. Economic incentives and technological capabilities of online platforms to maximise engagement have also helped amplify emotionally and politically resonant messages. Due to the potential to monetise engagement, influencers have an incentive to produce

provocative and controversial content. Such “attention hacking” aims to increase the visibility of content through the strategic use of social media, memes, and bots. As influencers and digital marketers work with engagement metrics, they learn that controversial and emotional responses are highly engaging and tend to go viral (Marwick and Lewis, 2017^[14]; Diaz Ruiz, 2023^[15]) (Tellis et al., 2019^[16]). Such content often makes it harder to differentiate authentic or quality information and facilitates malign actors’ efforts – domestic or foreign-born – to spread manipulated and intentionally false or misleading content. Ultimately, these changes have affected trust.

The development of the use of generative Artificial intelligence is yet another emerging challenge. A study last year found that humans are almost incapable of differentiating AI from human generated news in 50% of cases (Lorenz, Perset and Berryhill, 2023^[17]). Generative AI amplifies the risk of mis- and disinformation because it can produce false or misleading information that appears credible, and because it can do so at scale. Generative AI capabilities can also be abused to combine image, video, voice and text to create manipulated images or videos of public figures, or to target women or marginalised populations. Enabling the creation of targeted content to specific groups, such as minority communities, or age, gender, professional, and socio-economic groups, can aim to create dissent and fuel polarisation and further magnify the challenges that public debate on digital platforms pose (Lorenz, Perset and Berryhill, 2023^[17]).

The changes in how people receive and share information are taking place alongside – and are helping contribute to – fundamental changes in the public’s relationships with government and other civic institutions. The demand for deceptive content often reflects larger threats to democracy. Low voter turnout, increasing political polarisation and greater disengagement of citizens from politics represent growing challenges for policymakers (OECD, 2022^[11]). Only four in ten respondents (41.4%) to the OECD’s 2021 Trust Survey trust their national government. This data mirrors suspicion toward traditional media; around four out of ten (41.4%) respondents to the OECD’s 2021 trust survey say they do not trust the news media, though the results vary across countries and reflect specific cultural and social contexts (OECD, 2022^[18]). This context highlights the importance of focusing on strengthening trust in institutions in tandem with the fight against

disinformation in an effort to break a cycle in which malign actors exploit the lack of trust for their own gains.

Reinforcing democracy, a key priority for the OECD, must therefore incorporate a range of strategies and approaches to build trust and facilitate public engagement in democratic debates and policy-making. Ensuring individuals have a strengthened role in public decision-making also depends upon efforts to protect and promote civic space (both online and offline) which can play a key role in tackling disinformation and needs to be protected from online harassment and disinformation (OECD, 2022^[19]).²

1.3. DEMOCRATIC GOVERNMENTS' ROLE IN REINFORCING INFORMATION INTEGRITY RATHER THAN FOCUSING ON CONTENT

Combined with the continued and increasing importance of online platforms with a global audience, new governance models are needed to ensure information ecosystems that can support democratic debate (OECD, 2022^[18]). Despite consensus around the challenges posed by the spread of mis- and disinformation, democracies struggle to counter it while protecting freedom of expression and the ability to access free, diverse, and reliable information. Maintaining fundamental civic freedoms and an open Internet means that mis- and disinformation will never fully disappear (OECD, 2022^[19]). Since it is not governments’ role to “govern information” or serve as “arbiters of truth”, a comprehensive approach to instilling checks and balances in the information ecosystem needs to go beyond tackling only disinformation itself. The aim, rather, is for governments to create the conditions for an information ecosystem that safeguards information integrity.

The term “information integrity” is used in various fields, including journalism, computer science, information systems, data management, and cybersecurity. While the definitions in these fields are not entirely applicable to information ecosystems in democracies, the objectives in these sectors can be informative. For example, across data systems, information integrity can refer to the importance of maintaining the quality, consistency, clear provenance, and reliability of information. The term ‘integrity’ in this case refers to guarding against improper modification or destruction of content, as well as ensuring information authenticity (Barker, 2003^[20]).

The objective to reinforce information integrity in democratic societies is driven by the foundational aim of upholding fundamental freedoms, including freedom of expression and reinforcing democracy. Efforts to build information integrity should therefore include not only addressing sector- or technology-specific concerns, but also respond to the challenges facing the media and information ecosystems and democracy at large. The global nature of the challenges will require a strong global coalition of like-minded countries to work together to create environments that promote more accurate, trustworthy, and reliable information and that support the larger effort to reinforce democracy.

A more comprehensive and positive focus also helps respond to the challenges inherent in classifying content. Disinformation itself – and even more broadly, false, or misleading content – is different from other kinds of content that democracies regulate. For example, most democracies have made illegal clear and credible personal threats, incitement to violence, child pornography, terrorist content, fraud, copyright violations, misleading advertising, libel, and image rights as types of content that are identifiable and that pose a specific threat to democratic discourse, to individual rights or to intellectual property rights.

Increased attention to the threat posed by disinformation has prompted governments to adopt regulations around online mis- and disinformation, including by requiring additional responsibilities for platforms to make content-specific moderation decisions. Indeed, between 2016-2022, 91 laws worldwide were enacted or amended to include provisions regarding false or misleading information (Lim and Bradshaw, 2023^[21]). What makes content-specific regulatory responses particularly complex is not only that defining what content may be restricted without infringing upon freedom of expression is difficult, but also that illiberal regimes can co-opt laws to combat disinformation developed in countries with effective checks and balances to legitimise their own anti-democratic practices (Lim and Bradshaw, 2023^[21]).

Identifying the accuracy of information is often challenging. While it might prove relatively easy to identify certain types of misleading content (such as doctored photographs), distinguishing accurate from misleading or false assertions is complex even in relatively objective or scientific topics, as the evolving

understanding around how COVID-19 spreads and the effectiveness of face masks showed (see discussion of the role of fact-checkers in Chapter III). Doing so can be particularly complicated in fields related to social sciences and is particularly problematic in political discourse contexts (Del Campo, 2021^[22]).

While states have a role in enforcing existing rules in the information space – such as those that seek to promote independent, plural, and quality traditional media, as well as in defining illegal content per the constraints of their constitutional system – regulation of ‘legal but harmful’ content is inherently challenging (Douek, 2021^[23]). Indeed, UN human rights bodies have highlighted that “criminalising disinformation is inconsistent with the right to freedom of expression” (Rikhter, 2019^[24]). Special rapporteurs on freedom of expression have likewise issued several declarations noting that overly broad and vague laws purporting to combat misinformation often run afoul of international human rights standards.³

A challenge posed by disinformation-specific content laws is that while they emphasise takedowns and removals of “disinformation”, they suffer from problems of poor definitions of what constitutes false or misleading content (OHCHR, 2021^[25]). Vague definitions that are subject to a wide range of interpretations can give governments the power to selectively target content, resulting in varying levels of enforcement and inconsistent or politically motivated sanctions. Even if not abused by the regulator to unduly limit speech, overly broad content-specific laws may also incentivise platforms themselves to take down more than the law requires if they face unclear legal liability for hosting user speech (Douek, 2021^[23]). Given that moderation decisions of private platforms will have the potential to extend far beyond the limits of a government’s constitutional power to regulate speech, increasing the incentives for private companies to take a strict approach to content moderation may in effect increase censorship by proxy, reiterating the importance of strong freedom of expression protections (Keller, 2017^[26]).

Ultimately, poorly targeted or vague content-specific regulations risk unduly restricting speech. Particularly given the difficulties in defining what is meant by “disinformation”, this context points to the need to develop a positive, but not intrusive, vision for governance responses focused on information integrity.

1.4. CONSIDERATIONS AND PATH FORWARD

The challenges faced cannot be blamed solely on online platforms or new technologies, and any solutions will require focusing on strengthening democratic governance. A policy framework that creates information systems that upholds freedom of expression, focuses on processes rather than on content, and seeks to build societal resilience rather than silence voices.

A wide range of actors have developed a growing set of codes of practice, guidelines, and voluntary and self-regulatory mechanisms to promote this effort, but these mechanisms alone are insufficient. Despite progress, voluntary codes of practice and principles are limited by the extent to which private actors choose to comply. In this context, governments have a key role to play. The OECD's policy framework for government responses therefore encompasses a range of options to counter disinformation and strengthen information integrity. Building information integrity is by its nature a long-term process, though it also requires governments to respond to immediate threats and increasingly sophisticated disinformation campaigns; both short-term and longer-term responses will form the range of relevant efforts.

The framework will also help identify how to measure policy impact and success in improving information integrity. A comprehensive approach will include a broad range of measures; deploy them together with a continuous effort to assess, address, and avoid the threats and harm caused by mis- and disinformation; and evaluate initiatives with a close attention to potential impacts on freedom of expression (OECD, 2022^[11]). In this way, the OECD framework will also lay the groundwork for identifying future international standards and policy guidelines that help countries design, implement, and measure policy efforts to building information integrity. Note that policies in this space also often refer to regulatory responses, depending on the country context.

It also needs to be acknowledged that in a growing number of countries, the democratic premises on which this framework builds are not, or only partially, in place. At the same time, these countries are often more vulnerable to disinformation campaigns, and some of them may also use government resources to develop

and deploy such campaigns. Tackling disinformation and building information integrity in such contexts can be inspired by this framework, though will require tailored strategies. A compromised information ecosystem limits the public's access to quality information, thereby reducing trust and engagement in democratic life and reducing awareness of educational, health, and economic opportunities. To that end, reinforcing information integrity globally will require framing the subject through the human rights, social, and economic implications relevant for people's lives.

To that end, a comprehensive overview to help guide actions could focus on the following elements:

1.4.1. Implementing policies to enhance the transparency, accountability, and plurality of information sources

Digital communications and online platforms have altered how information is created and shared and altered the economic models that underpin the information space. Online platforms have facilitated the spread of polarising, sensational, and false or misleading information, while operating in nascent regulatory environments. The global reach of these platforms surpasses national (and even supra-national) regulatory jurisdictions. At the same time, voluntary self- and co-regulatory regimes are limited in that they allow some actors to sidestep obligations, underscoring the importance of government involvement in designing, enforcing, and updating regulatory responses, as appropriate.

Done appropriately and with the aim of supporting democratic engagement, the health, transparency, and competitiveness of information spaces can be supported by appropriate, effective, and agile policymaking. To that end, policies to promote the transparency and accountability of online platforms are an option to help build understanding of their business-models and the related risks to democratic processes, help mitigate threats, including those posed by foreign information manipulation and interference, and foster healthier information spaces.

In addition to focusing on online platforms, a strong, pluralistic, and diverse media sector with solid journalists is a foundation for reinforcing information integrity and an essential component of democracy. Reinforcing information integrity will require promoting

the transparency and health of these spaces through effective design, monitoring, and implementation of relevant policies. By providing sources of fact- and evidence-based content informed by standards of professional quality, journalists and the media sector more widely – including national, local, and community outlets and multiple on- and offline sources – can counter the impact of mis- and disinformation and inform public debate in democracy. The role of these sources of news and information in democracies, however, continues to face changes and challenges exacerbated by the development of online communication technologies and the role social media platforms have played in shaping the information environment.

To that end, the emerging understanding suggests that governments should pursue the following objectives to strengthening the positive role of media and online platforms in the information space:

- Uphold a free, independent, and diverse media sector as an essential component of open and democratic societies. In addition to the legal foundation for ensuring freedom of opinion and expression, governments must protect journalists, media workers, and researchers, and monitor, investigate, and provide access to justice for threats and attacks against them. Adopting national action plans for the safety of journalists, engaging with press councils and mapping and monitoring risks and threats are additional actions that can be taken.
 - Design policies to reinforce a diverse, pluralistic, and independent market for traditional media. Limiting market concentration, promoting transparency and diversity of media, and mandating editorial independence can all play an important role in preventing undue influence from political and commercial interests.
 - Support independent and high-quality public service media. These outlets are often among the most trusted sources of news and can play an important role in democracies as providers of independent, quality, and trusted news and information.
 - Explore direct and indirect financial support – including special taxation regimes and targeted funding – to media outlets that meet specified criteria and help achieve democratic objectives,
- such as reinforcing local, community, cultural, minority language, or investigative journalism. Governments should also recognise the distinct nature of not-for-profit community media and guarantee their independence. Reinforcing a diverse and independent media sector is also an important component for international support and overseas development assistance. Throughout these efforts, however, governments should put in place clear and transparent rules for funding allocation, and provide information about subsidies, financing, and project activities. Such processes should be designed to show and ensure that governments have no direct impact on content development, and to help prevent political bias in funding selection.
 - Avoid unduly restricting speech through overly broad content-specific regulations that do not meet stringent, transparent, and objectively defined criteria that are consistent with the State's international human rights obligations and commitments. This is particularly important given the difficulties in defining "disinformation" and that legislating "legal but harmful" content risks limiting speech.
 - Recognise the role that intermediary liability protections play in fostering a free and open internet and in balancing platforms' responsibilities to address legitimate concerns around false, misleading, and otherwise harmful or illegal content.
 - Increase transparency and responsibility, including, where relevant, through regulatory efforts, of relevant actors to better understand and mitigate potential and actual impacts of generative AI tools with respect to disinformation. Such an approach will be particularly important given the novelty, rapid evolution, and uncertainty related to how and to what extent these new technologies will amplify the challenges of trust in the information space. Understanding the principles used to guide the development and application of generative AI tools; increasing transparency of the data sets used in their design; watermarking AI generated content; and requiring testing, risk identification and mitigation, and monitoring will help build trust. At the same time, restricting uses of deepfakes

in some specific and well-defined contexts, such as in processes related to election administration, might help mitigate the threat posed by false and misleading content.

- Enhance transparency and information sharing around policies, policy development, processes, and decisions of online platforms to enable better understanding of their operations and impacts of business models, risk mitigation measures, and algorithms, as appropriate. Putting in place mechanisms, including regulatory mechanisms, as appropriate, to increase platform disclosures related to their terms of service, efforts to prevent and address human rights impacts, and privacy policies; procedures, guidelines, and tools that inform the content moderation and algorithmic decision making; and complaint handling processes can empower users to better understand data handling and rule enforcement. This information can also encourage platform accountability to users, as public scrutiny can reinforce positive actions to address adverse impacts while highlighting potential biases, human rights risks, or unfair practices. Facilitating the standardisation of such information can also encourage the creation of best practices for policy development and inform ways to measure the impact of those interventions.
- Facilitate greater access to data for academics and other researchers that helps build understanding of how content spreads across platforms and throughout information spaces, including through regulatory requirements, as appropriate. Analysing public data (not private posts or messages) that does not include personally identifiable information could also generate insights into online behaviour, patterns, and changes over time, thereby facilitating impact assessments of policies. Enabling governments and independent researchers to verify and confirm platforms' public disclosures, including around political advertising, can also promote accountability. Promoting standardised reporting mechanisms, mandating that steps are taken to ensure research is conducted for legitimate aims, and that researchers implement privacy and security

protections will be important efforts to ensure quality research and to help prevent abuse.

- Apply policies to counter foreign malign interference to the information space. Applying existing policies designed to counter foreign interference, when they exist and as appropriate, to online communication technologies is a useful avenue to build trust. By making the identity of foreign agents and owners of media outlets known, such schemes can help illuminate covert and potentially malign communication activities.
- Safeguard information integrity in times of democratic elections. Putting in place mechanisms to monitor specific threats and to provide timely and reliable information to citizens to enable them to exercise their rights will be key in this fast-changing information environment. Readily available, high-quality information that is tailored for specific at-risk communities regarding identified threats will enable governments to prevent information gaps that can be exploited by disinformation propagators.
- Identify economic drivers that encourage new entrants, innovation, and data portability to spur competition between online platforms, potentially encouraging market-based responses to support better functioning information spaces.

1.4.2. Fostering societal resilience to disinformation

Strengthening participation by and engagement with the public, civil society, and media workers will be essential as countries look to strengthen information integrity, reinforce democracy, and build trust. A whole-of-society approach, grounded in the protection and promotion of civic space, democracy, and human rights, will be necessary given the fundamental role that individuals and non-governmental partners have in promoting information integrity.

Notably, citizens and stakeholders often have relevant and needed experience, human capital, and qualifications that can provide complementary perspective to governmental policymaking and to identify and respond to disinformation threats. Non-government actors may also have easier access to and

greater experience working with groups that governments cannot reach as easily, for example, migrants, diasporas, and other minority, marginalised, or socially excluded groups who may be particularly affected by targeted disinformation. To the extent that non-governmental actors are seen as more reliable sources of trustworthy information than governmental institutions, the public may also be more receptive to projects and other initiatives managed by civil society organisations.

Governments are advancing steadily in this area, increasingly putting in place frameworks for successful engagement and partnership with the public and non-government partners, recognising that groups have different needs. As governments develop multi-stakeholder approaches, they should be guided by the following questions:

- How can participatory initiatives that engage citizens and non-government stakeholders be best designed and carried out to build understanding of the information space and develop effective policy responses?
- What are the benefits and potential drawbacks of partnerships and collaboration with non-government partners, including the private sector? How can any drawbacks or risks – to government and non-government partners – be mitigated?
- How can governments best decide which initiatives to strengthen information integrity should be carried out in partnership with CSOs, media, academia, the private sector (not only online platforms) and where can – or should – governments act alone?
- How can whole-of-society efforts designed to strengthen information integrity be measured to track their effectiveness and value?

To that end, governments should consider the following efforts to pursue a whole-of-society approach to strengthening societal resilience and citizen and stakeholder participation:

- Enhance public understanding of – and skills to operate in – a free information space conducive to democratic engagement. Governments should ensure that civic, media, and digital information literacy, education and initiatives form part of a broader effort to build societal resilience and measure the effectiveness of

initiatives. Promoting media and information literacy in school curricula from primary and secondary school to higher education, developing training programmes for teachers, conducting impact evaluations of media and information literacy programmes (including longitudinal studies), as well as supporting research to better understand the most vulnerable segments of the population to the risk of disinformation and to better target media and information programmes should form key pillars of governments' toolbox.

- Implement information access laws and open government standards, including publicly accessible open data, to lower barriers for journalists and citizens to access public information and officials.
- Build capacity and work with partners from across society (notably academics, CSOs, media, and online platforms) to monitor and evaluate changes to and policy impacts on the information space. Beyond output measurements, methods for understanding the impact of disinformation and counter-disinformation efforts should also include monitoring changes in broad indicators over time, such as behavioural indicators and susceptibility to mis- and disinformation narratives.
- Provide clear and transparent guidelines and oversight mechanisms for government engagement with other actors, to ensure that when governments are partnering with, funding, or otherwise co-ordinating with or supporting activities of non-government partners on issues related to information integrity governments cannot unduly influence the work of these actors or restrict freedom of expression. Unclear rules, exclusions, or decisions could create distrust in the process. Such guidelines and oversight mechanisms are particularly valuable in avoiding actual and perceived politicisation of governments' engagement with non-government actors.
- Build the capacity of the still largely underdeveloped public communication function to play a constructive role in supplying timely information and in raising awareness of threats, while developing a more solid governance for its own functioning, away from

politicised information. In the short-term, the function can serve as an important source of information, including in times of crisis. Over the longer-term, building the capacity of the function to provide citizens with the skills necessary to better understand the information environment, for example through pre-bunking, can be an important tool for societal resilience.

- Strengthen mechanisms to avoid real or suspected conflict of interest with respect to the public communication function. Transparent, accountable, and professional management of the public communication function can help ensure it plays an important role in providing timely information that can build awareness of relevant challenges and threats and provide proactive communication that helps build societal resilience to the spread of disinformation.
- Expand understanding of the information space by supporting research activities to better understand trends in information and content consumption patterns, the threats posed and tactics used by foreign actors spreading false and misleading information, and methodologies for assessing the impact of risk mitigation measures. Strengthen opportunities and mechanisms for research to inform the policy-making process.
- Design and put in place effective participatory mechanisms with citizens, journalists, social media platforms, academics, and civil society organisations to help establish policy priorities and clarify needs and opportunities related to strengthening information integrity. Building more meaningful democratic engagement, including through deliberative citizens assemblies, around policy design and implementation as related to information integrity will contribute to broader efforts to strengthen democracy resilience.
- Identify government collaboration on information integrity with non-government partners, including journalists, academia, the private sector, and other relevant non-governmental organisations. Engagement activities and outputs, including those related to funding, the goals of the co-operation, and impact on content decisions, should be clearly identifiable by the public. Similarly, the public

should be able to identify whether a communication campaign, media literacy activity, or research product is financed or guided by government institutions.

- Take steps to clarify funding sources to mitigate the risks of malign interfering groups gaining access to data or being able to manipulate a country's information space.
- Mitigate the risk to governmental staff, academics, CSOs, private sector, and other actors engaged in information integrity initiatives when they become targets of disinformation campaigns, other threats, and harassment. When necessary, enable appropriate measures to protect the human rights of affected individuals.

1.4.3. Upgrading governance measures and institutional architecture to uphold the integrity of the information space

Governments have increasingly recognised the need to put in place accountable, transparent, and agile governance processes and structures as they seek to develop effective responses to the threats posed by disinformation and reinforce information integrity. Effectiveness, as it relates to governance responses within democracies, is not merely about countering disinformation. More broadly, effectiveness refers to information ecosystems that are free, diverse, and transparent and that create the conditions for citizens to make well-informed decisions and engage in constructive civic dialogue, while protecting the human rights of all. These efforts will be most effective if they are focused on diversity and inclusivity from the bottom up, including in staffing, strategic planning, and partnerships. This will help to bring in individuals with the right set of skills and experiences to tackle some of the most pressing topics in information integrity.

To this end, governments will need to adapt and upgrade their institutional architecture by pursuing the following objectives, as appropriate:

- Develop and implement strategic frameworks that support a coherent vision and a comprehensive approach to reinforce information integrity. This guidance can be articulated via national strategies that specifically focus on disinformation and information integrity, or included as part of

other official documents, such as national strategies on defence and security, digitalisation, public communications, or culture and education. Effective strategic frameworks describe objectives, the time frame and scope of action, and operational aspects around institutional setting, reporting, and evaluation processes. Further analysis will help identify trends and best-practices to enhance the role of strategic guidance in this space.

- Establish clearly defined offices, units, or co-ordination mechanisms to promote mutually supporting actions across government bodies in charge of addressing mis- and disinformation threats and reinforcing information integrity. A well co-ordinated multi-agency approach can help countries make connections to sectoral priorities, enable prompt information-sharing, and avoid duplication of efforts between institutional authorities. Governments may also consider creating task forces to provide expert advice on policies related to technical dimensions of disinformation, such as hybrid threats, foreign interference, and electoral interference. A multi-agency approach will also help align short-term needs, such as information provision related to crises, elections, or immediate threats, with longer-term objectives related to building information integrity and societal resilience. Prioritise building mechanisms for effective communication and information sharing and the building of relationships among staff within and across entities. Enable an evidence-driven culture that incorporates measurement and evaluation of each stage of the policy development and implementation process.
- Outline the functioning and objectives of relevant offices and units in legal provisions that define the mandate and the parameters within which they operate. These provisions are important to establish accountability and reporting procedures and to help ensure that government activities do not infringe on fundamental rights and freedoms.
- Enhance international co-operation to strengthen the democratic response to challenges in the information space via partnerships, alliances, and by connecting and enabling existing networks across different sectors. Sharing strategic intelligence, analytical methodologies, as well as policy responses and their results can help draw on relevant lessons and identify best-practices.
- Provide capacity-building opportunities at the local, national, and international level for public officials who address relevant challenges in their daily work. The level of sophistication of disinformation campaigns requires training and upskilling at all levels of government to ensure that public administrators and policymakers have the knowledge and tools to recognise, monitor, and counter the spread of false and misleading information without impinging on freedom of expression. Promote diverse workforces and cultures of inclusivity; these are not only core democratic values, but also a cornerstone to enabling effective countermeasures to disinformation and its impact, due to the multidisciplinary nature of the problem and solutions.
- Implement agile regulatory policy responses to the challenges introduced by emerging communication technologies. Particularly in the information space, which is characterised by novel forms of communication that blur traditional delineations between regulated sectors, regulatory policy should adapt and learn throughout the cycle, including with improved co-ordination between authorities to reduce fragmented government responses. Governments should put in place mechanisms for public and stakeholder engagement in the regulatory process; implement comprehensive regulatory Impact Assessments (RIA) processes; conduct impact evaluation and monitoring; evaluate proper audit and enforcement mechanisms and authorities; and conduct timely and proportionate re-evaluation of relevant regulations.
- Increase the capacity of regulatory oversight and advisory bodies to anticipate the evolution of the information ecosystem and implement strategic foresight that informs the design, implementation, and analysis of regulations. Building regulators' capacity and flexibility will also facilitate experimentation, including in the form of regulatory sandboxes, so that resulting frameworks are more adaptive.

- Strengthen international regulatory co-operation to avoid fragmentation and prevent regulatory arbitrage. Given the inherently global nature of online information flows, co-operation among governments and policymakers is essential to ensure the effectiveness, efficiency, coherence, and continued relevance of regulatory policies and frameworks.

REFERENCES

- Barker, W. (2003), *Guideline for Identifying an Information System as a National Security System*, National Institute of Standards and Technology, [20]
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf>.
- Diaz Ruiz, C. (2023), "Disinformation on digital media platforms: A market-shaping approach", *New Media & Society*, [15]
<https://doi.org/10.1177/14614448231207644>.
- Douek, E. (2021), "Governing Online Speech: From "Posts-as-Trumps" to Proportionality and Probability", [23]
Columbia Law Review, Vol. 121/No. 3, <https://columbialawreview.org/content/governing-online-speech-from-posts-as-trumps-to-proportionality-and-probability/>.
- Feldstein, S. (ed.) (2021), *Disinformation Is Not Simply a Content Moderation Issue*, Issues on the Frontlines of Technology and Politics, Carnegie Endowment for International Peace, [22]
<https://carnegieendowment.org/2021/10/19/disinformation-is-not-simply-content-moderation-issue-pub-85514>.
- Government of the Netherlands (2023), *Global Declaration on Information Integrity Online*, [9]
<https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2023/09/20/global-declaration-on-information-integrity-online>.
- Gupta, M., C. Parra and D. Dennehy (2021), "Questioning racial and gender bias in AI-based recommendations: do espoused national cultural values matter?", *Information Systems Frontiers*, pp. 1-17, [7]
<https://doi.org/10.1007/s10796-021-10156-2>.
- Jensen, K. and R. Helles (2017), "Speaking into the system: Social media and many-to-one communication", *European Journal of Communication*, Vol. 32/1, pp. 16–25, [12]
<https://doi.org/10.1177/0267323116682805>.
- Keller, D. (2017), *Making Google the Censor*, <https://www.nytimes.com/2017/06/12/opinion/making-google-the-censor.html?smprod=nytcore-ipad&smid=nytcore-ipad-share&r=0>. [26]
- Leshner, M., H. Pawelec and A. Desai (2022), *Disentangling untruths online: Creators, spreaders and how to stop them*, Going Digital Toolkit, OECD Publishing, Paris, [4]
https://goingdigital.oecd.org/data/notes/No23_ToolkitNote_UntruthsOnline.pdf.
- Lim, G. and S. Bradshaw (2023), *Chilling Legislation: Tracking the Impact of "Fake News" Laws on Press Freedom Internationally*, Center for International Media Assistance, [21]
https://www.cima.ned.org/publication/chilling-legislation/#cima_footnote_3.
- Lorenz, P., K. Perset and J. Berryhill (2023), "Initial policy considerations for generative artificial intelligence", *OECD Artificial Intelligence Papers*, No. 1, OECD Publishing, Paris, [17]
<https://doi.org/10.1787/fae2d1e6-en>.

- Marwick, A. and R. Lewis (2017), "Media Manipulation and Disinformation Online", *Data & Society*, [14]
<https://datasociety.net/library/media-manipulation-and-disinfo-online/>.
- OECD (2022), *Building Trust and Reinforcing Democracy: Preparing the Ground for Government Action*, [1]
 OECD Public Governance Reviews, OECD Publishing, Paris, <https://doi.org/10.1787/76972a4a-en>.
- OECD (2022), *Building Trust to Reinforce Democracy: Main Findings from the 2021 OECD Survey on Drivers of Trust in Public Institutions*, Building Trust in Public Institutions, OECD Publishing, Paris, [18]
<https://doi.org/10.1787/b407f99c-en>.
- OECD (2022), "Declaration on Building Trust and Reinforcing Democracy", *OECD Legal Instruments*, [10]
 OECD/LEGAL/0484, OECD, Paris, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0484>.
- OECD (2022), *The Protection and Promotion of Civic Space: Strengthening Alignment with International Standards and Guidance*, OECD Publishing, Paris, [19]
<https://doi.org/10.1787/d234e975-en>.
- OECD (2021), *OECD Report on Public Communication: The Global Context and the Way Forward*, OECD [5]
 Publishing, Paris, <https://doi.org/10.1787/22f8031c-en>.
- OHCHR (2021), *Moderating online content: fighting harm or silencing dissent?*. [25]
- Reuters Institute for the Study of Journalism (2022), *The changing news habits and attitudes of younger audiences*. [13]
- Rikhter, D. (2019), *International Standards and Comparative National Approaches to Countering Disinformation*, OSCE. [24]
- Southwell, B., E. Thorson and L. Sheble (eds.) (2018), *Misinformation and Mass Audiences*, University of [11]
 Texas Press, <https://doi.org/10.7560/314555>.
- Tellis, G. et al. (2019), "What drives virality (sharing) of online digital content? The critical role of [16]
 information, emotion, and brand prominence", *Journal of Marketing*, Vol. 83/4, pp. 1-20.
- U.S. Department of State (2023), *How the People's Republic of China Seeks to Reshape the Global [2]
 Information Environment*, <https://www.state.gov/gec-special-report-how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/>.
- Wardle, C. and H. Derakshan (2017), *Information Disorder: Towards an interdisciplinary framework for [3]
 research and policy making*, <http://tverezo.info/wp-content/uploads/2017/11/PREMS-162317-GBR-2018-Report-desinformation-A4-BAT.pdf>.
- Westerwick, A., B. Johnson and S. Knobloch-Westerwick (2017), "Confirmation biases in selective exposure [6]
 to political online information: Source bias vs. content bias", *Communication Monographs*, Vol. 84/(3), pp. 343–364.
- Zhao, H., S. Fu and X. Chen (2020), "Promoting users' intention to share online health articles on social [8]
 media: The role of confirmation bias .", *Information Processing & Management*, Vol. 57(6), <https://doi.org/10.1016/j.ipm.2020.102354>.

NOTES

¹ Misinformation is sometimes used as a catchall term for many similar but ultimately different practices, for example disinformation, information influence operation, and foreign interference in the information space, each of which may require a different approach. Mis- and disinformation are furthermore not to be confused with the dissemination of terrorist, violent, or illegal content online (OECD, 2022^[1]).

² For additional information, see the OECD Action Plan on Enhancing Representation, Participation and Openness in Public Life (October 2022) <https://www.oecd.org/governance/oecd-luxembourg-declaration-action-plan-enhancing-representation-participation-and-openness-in-public-life.pdf>.

³ As noted in (Lim and Bradshaw, 2023^[21]), language on the risks that content-specific legislation poses can be found: “Disinformation and Freedom of Opinion and Expression: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Irene Khan,” United Nations General Assembly, April 13, 2021, <https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/HRC/47/25&Lang=E>; “Joint Declaration on Freedom of Expression and ‘Fake News’, Disinformation and Propaganda,” OSCE, March 3, 2017, www.osce.org/files/f/documents/6/8/302796.pdf; “Twentieth Anniversary Joint Declaration: Challenges to Freedom of Expression in the Next Decade,” United Nations Human Rights Office of the High Commissioner, July 10, 2019, www.ohchr.org/sites/default/files/Documents/Issues/Opinion/JointDeclaration10July2019_English.pdf; “Joint Declaration on Freedom of Expression and Elections in the Digital Age,” United Nations Human Rights Office of the High Commissioner, April 30, 2020, www.ohchr.org/sites/default/files/Documents/Issues/Opinion/JointDeclarationDigitalAge_30April2020_EN.pdf.



From:
**Facts not Fakes: Tackling Disinformation,
Strengthening Information Integrity**

Access the complete publication at:

<https://doi.org/10.1787/d909ff7a-en>

Please cite this chapter as:

OECD (2024), "Introduction: Toward a comprehensive framework for countering disinformation and reinforcing information integrity", in *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity*, OECD Publishing, Paris.

DOI: <https://doi.org/10.1787/cc7a7a39-en>

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area. Extracts from publications may be subject to additional disclaimers, which are set out in the complete version of the publication, available at the link provided.

The use of this work, whether digital or print, is governed by the Terms and Conditions to be found at <http://www.oecd.org/termsandconditions>.