Facts not Fakes

TACKLING DISINFORMATION, STRENGTHENING INFORMATION INTEGRITY

OECD

Facts not Fakes

TACKLING DISINFORMATION, STRENGTHENING INFORMATION INTEGRITY

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.

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

Note by the Republic of Türkiye

The information in this document with reference to "Cyprus" relates to the southern part of the Island. There is no single authority representing both Turkish and Greek Cypriot people on the Island. Türkiye recognises the Turkish Republic of Northern Cyprus (TRNC). Until a lasting and equitable solution is found within the context of the United Nations, Türkiye shall preserve its position concerning the "Cyprus issue".

Note by all the European Union Member States of the OECD and the European Union

The Republic of Cyprus is recognised by all members of the United Nations with the exception of Türkiye. The information in this document relates to the area under the effective control of the Government of the Republic of Cyprus.

Please cite this publication as:
OECD (2024), *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity*, OECD Publishing, Paris, https://doi.org/10.1787/d909ff7a-en.

ISBN 978-92-64-98010-5 (print)
ISBN 978-92-64-37311-2 (pdf)
ISBN 978-92-64-66050-2 (HTML)
ISBN 978-92-64-94902-7 (epub)

Photo credits: Cover © Rawpixel/Shutterstock.com.

Images © michaeljung/Shutterstock.com; © Master1305/Shutterstock.com; © Gorodenkoff/Shutterstock.com; © Sharomka/Shutterstock.com; © r.classen/Shutterstock.com; © Monkey Business Images/Shutterstock.com; © Arsenii Palivoda/Shutterstock.com; © DW labs Incorporated/Shutterstock.com.

Corrigenda to OECD publications may be found on line at: www.oecd.org/about/publishing/corrigenda.htm.

Foreword

Informed individuals are the foundation of democratic debate and society. The accelerated spread of false or misleading information, often through deliberate disinformation campaigns by domestic or foreign actors, creates confusion and exacerbates polarisation, distorts public policy debates, and further deteriorates trust in government. In a fast-moving information landscape re-shaped by digitalisation, strengthening the integrity of information spaces and combating disinformation are thus urgent to strengthen the social fabric of open societies and reinforce democracy.

Against this backdrop, developing a comprehensive set of policies for governments to help ensure that individuals can access diverse, timely, well-researched, and fact-checked information is imperative. Yet, in addition to ensuring that governments can play such a constructive, yet not intrusive, role in meeting the ambition of reinforcing information integrity while safeguarding the independence and variety of content production, all actors in the information ecosystem need to shoulder responsibilities. To that end, a multi-stakeholder approach is required to address this complex global challenge.

The report *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity* presents an overview of policies that have been designed and implemented with the aim of supporting information integrity. This report explores the importance of taking a comprehensive approach, tailored to country contexts, that emphasises the need to create an environment for reliable information to thrive. It recognises that democracies are based on free expression and open and informed debate, and that actors must work together to meet these global challenges.

The report presents an analytical framework that focuses on three complementary policy aims: (i) enhancing transparency, accountability, and plurality of information sources; (ii) fostering societal resilience to disinformation; and (iii) upgrading governance measures and institutional architecture to uphold the integrity of the information space.

This report benefitted from extensive collaboration with the Steering Group and Expert Group on Public Governance Responses to Misinformation and Disinformation, who shared their good practices and experiences to advance toward greater integrity in the information space and drive implementation in their own countries. The report was approved and declassified for publication by the OECD Public Governance Committee via written procedure on 29 February 2024.

OECD
Reinforcing Democracy Initiative

Acknowledgements

This publication is the work of the OECD Directorate for Public Governance (GOV), under the leadership of Elsa Pilichowski, Director. It was prepared by GOV's Anti-Corruption and Integrity in Government Division, under the direction of Julio Bacio Terracino, Head of Division. The report was drafted by Craig Matasick, Nuria Villanova, and Liudas Zdanavicius, with contribution from Charles Baubion. The report benefitted from editorial assistance and was prepared for publication by Meral Gedik.

The draft report was sent to and benefited from comments from Members of the OECD Public Governance Committee (PGC), as well as the OECD Steering Group and the Expert Group on Public Governance Responses to Mis- and Disinformation. Colleagues from GOV's Regulatory Policy; Innovative, Digital and Open Government; and Public Management and Budgeting Divisions provided feedback. OECD Directorates of Science, Technology and Innovation; Education and Skills; Development Co-operation; and Financial and Enterprise Affairs also provided comments.

The draft report received contributions from organisations, including the Forum on Information and Democracy, as well as experts including David Colon, Associate Professor and Researcher at the Department of History of the Paris Institute of Political Studies, and Paul-Joel Kamtchang, Executive Secretary of ADISI-Cameroon. It was also informed by the deliberations of representatives of governments, media and journalists, civil society, academia and the private sector who shared their insights during the public conference *Tackling disinformation: Strengthening democracy through information integrity*, held at OECD headquarters in November 2023 and on several other occasions.

Table of contents

FIGURES

BOXES

Executive summary

In democratic societies, characterised by freedom of speech and open debates as a way of reaching consensus at all levels of society, the search for information integrity is key to the ability of societies to hold together. Access to diverse sources of information, multiple and independent news sources, and free and open discourse are all needed to enable informed democratic debate.

It is now widely acknowledged that the spread of false and misleading information, at times deliberately disseminated to deceive or mislead, blurs public debates and fuels polarisation, eroding the social fabric of open societies more widely. Experiences that have only accelerated in recent years show that disinformation campaigns, strategically orchestrated by domestic or foreign actors, can have far-reaching consequences in many policy areas ranging from public health to national security or addressing the climate crisis. They cast doubt on factual evidence and aggravate existing societal divisions, making it difficult to build the societal consensus essential to address complex policy challenges.

Disinformation is not new phenomenon, but digitalisation has fundamentally changed its reach and impact. Communication technologies now allow for anyone with an internet connection to produce and distribute content, but without the responsibility to adhere to journalistic or academic and scientific ethics and standards, long built to favour information integrity.

While this increased accessibility provides unprecedented access to knowledge, can foster citizen engagement and innovative news reporting, it also provides a fertile ground for the rapid spread of false and misleading information. The development of the use of generative Artificial Intelligence will magnify this challenge even further.

On the supply side, the economic incentives of virality and recommendation algorithms frequently prioritise the value of information as a commodity, rather than a public good. This comes at the expense of quality journalism, already facing increasing economic pressures and high-risk environments. On the demand side, these new technologies increasingly respond to the psychological and behavioural drivers that underpin how people search for, process, and consume information.

Many countries have started examining the adequacy of existing policies and institutions that are in place to effectively address current and future realities of a rapidly evolving information environment. Action is required to counteract the threat posed by rising disinformation; at the same time, this action must not lead to greater information control in our democracies.

This new reality has acted as a catalyst for governments to explore more closely the constructive roles they can play in reinforcing the integrity of the information space – namely, how to support 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. Upholding information integrity is essential to safeguarding freedom of expression, including the freedom to seek, receive, and impart information and ideas.

Countries' growing appreciation for the need to act in this new information environment highlights the need to urgently take stock of the emerging policy priorities and set a path for action. This report is therefore a first baseline assessment that presents how governments are upgrading their governance measures and institutional architecture to support an enabling environment where reliable information can thrive,

while ensuring the vigilant protection of freedom of expression and human rights. It also examines the synergies between different policy dimensions to provide a better understanding of the conditions that contribute to information integrity. While the report outlines countries' policy priorities and actions, it also seeks to advance the discussion on policy recommendations moving forward.

Although country contexts are different, the report highlights common areas of concern and action. First, governments can continue to shift their focus from *ad hoc* policies to counter disinformation threats to a more systemic approach that strengthens information integrity more broadly, relying on all actors of society. Governments need to ensure that their policies are co-ordinated, evidence-based, and regularly evaluated to measure their effectiveness. In this sense, it will be important to identify timeframes for policy action and evaluation. For instance, policy actions, such as responding to immediate disinformation crises, especially during election periods, should be developed in parallel with other policy responses, such as investing in societal resilience, aimed to address the root causes of the issue at stake.

Finally, as information flows know no borders, governments cannot solve this problem alone. Peer learning can contribute to better policies across democratic countries facing similar issues. In addition, strengthening information integrity will also require all actors on the frontlines of information systems – namely the private sector, media, academia, and civil society – to shoulder their responsibilities and act together in support of information integrity.

This report presents an analytical framework to guide countries in the design of policies, looking at three complementary dimensions:

- **Implementing policies to enhance the transparency, accountability, and plurality of information sources**: This includes promoting policies that support a diverse, plural, and independent media sector, with a needed emphasis on local journalism. It also comprises policies that may be utilised to increase the degree of accountability and transparency of online platforms, so that their market power and commercial interests do not contribute to disproportionately vehicle disinformation.
- **Fostering societal resilience to disinformation**: This involves empowering individuals to develop critical thinking skills, recognise and combat disinformation, as well as mobilising all sectors of society to develop comprehensive and evidence-based policies in support of information integrity.
- **Upgrading governance measures and public institutions to uphold the integrity of the information space:** This involves the development and implementation of, as appropriate, regulatory capacities, co-ordination mechanisms, strategic frameworks, and capacity-building programmes that support a coherent vision and approach to strengthening information integrity within the public administration, while ensuring clear mandates and respect for fundamental freedoms. It also involves promoting peer-learning and international co-operation between democracies facing similar disinformation threats.

The aim of this emerging framework is to advance the conversation and develop common language for practical policy guidance. By building understanding of what successful policy responses look like, this framework can play a constructive role in informing policy design and implementation, as well as serve as a baseline for measuring progress in this area.

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]); (Lesher, 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[1]). 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[1]). 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, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf. [20]

Diaz Ruiz, C. (2023), "Disinformation on digital media platforms: A market-shaping approach", *New Media & Society*, https://doi.org/10.1177/14614448231207644. [15]

Douek, E. (2021), "Governing Online Speech: From "Posts-as-Trumps" to Proportionality and Probability", *Columbia Law Review*, Vol. 121/No. 3, https://columbialawreview.org/content/governing-online-speech-from-posts-as-trumps-to-proportionality-and-probability/. [23]

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, https://carnegieendowment.org/2021/10/19/disinformation-is-not-simply-content-moderation-issue-pub-85514. [22]

Government of the Netherlands (2023), *Global Declaration on Information Integrity Online*, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2023/09/20/global-declaration-on-information-integrity-online. [9]

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, https://doi.org/10.1007/s10796-021-10156-2. [7]

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, https://doi.org/10.1177/0267323116682805. [12]

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]

Lesher, M., H. Pawelec and A. Desai (2022), *Disentangling untruths online: Creators, spreaders and how to stop them*, Going Digital Toolkit, OECD Publishing, Paris, https://goingdigital.oecd.org/data/notes/No23_ToolkitNote_UntruthsOnline.pdf. [4]

Lim, G. and S. Bradshaw (2023), *Chilling Legislation: Tracking the Impact of "Fake News" Laws on Press Freedom Internationally*, Center for International Media Assistance, https://www.cima.ned.org/publication/chilling-legislation/#cima_footnote_3. [21]

Lorenz, P., K. Perset and J. Berryhill (2023), "Initial policy considerations for generative artificial intelligence", *OECD Artificial Intelligence Papers*, No. 1, OECD Publishing, Paris, https://doi.org/10.1787/fae2d1e6-en. [17]

Marwick, A. and R. Lewis (2017), "Media Manipulation and Disinformation Online", *Data & Society*, https://datasociety.net/library/media-manipulation-and-disinfo-online/. [14]

OECD (2022), *Building Trust and Reinforcing Democracy: Preparing the Ground for Government Action*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/76972a4a-en. [1]

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, https://doi.org/10.1787/b407f99c-en. [18]

OECD (2022), "Declaration on Building Trust and Reinforcing Democracy", *OECD Legal Instruments*, OECD/LEGAL/0484, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0484. [10]

OECD (2022), *The Protection and Promotion of Civic Space: Strengthening Alignment with International Standards and Guidance*, OECD Publishing, Paris, https://doi.org/10.1787/d234e975-en. [19]

OECD (2021), *OECD Report on Public Communication: The Global Context and the Way Forward*, OECD Publishing, Paris, https://doi.org/10.1787/22f8031c-en. [5]

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 Texas Press, https://doi.org/10.7560/314555. [11]

Tellis, G. et al. (2019), "What drives virality (sharing) of online digital content? The critical role of information, emotion, and brand prominence", *Journal of Marketing*, Vol. 83/4, pp. 1-20. [16]

U.S. Department of State (2023), *How the People's Republic of China Seeks to Reshape the Global Information Environment*, https://www.state.gov/gec-special-report-how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/. [2]

Wardle, C. and H. Derakshan (2017), *Information Disorder: Towards an interdisciplinary framework for research and policy making*, http://tverezo.info/wp-content/uploads/2017/11/PREMS-162317-GBR-2018-Report-desinformation-A4-BAT.pdf. [3]

Westerwick, A., B. Johnson and S. Knobloch-Westerwick (2017), "Confirmation biases in selective exposure to political online information: Source bias vs. content bias", *Communication Monographs*, Vol. 84/(3), pp. 343–364. [6]

Zhao, H., S. Fu and X. Chen (2020), "Promoting users' intention to share online health articles on social media: The role of confirmation bias .", *Information Processing & Management*, Vol. 57(6), https://doi.org/10.1016/j.ipm.2020.102354. [8]

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.


Social Network
Events
Friends
Posts
Bookmarks
Products
Photos
Anna Hicks
Events
Halloween Party

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

This chapter provides an overview of policies to reinforce the ecosystem that promotes information integrity. It discusses policies encouraging responsibility and transparency of online and social media platforms and the imperative of countering specific risks in the information space, including foreign information manipulation and interference, the safeguarding of information integrity in times of democratic elections, and the changes introduced by generative AI to the information space. It also provides an overview of the essential role played by plural, independent, and sustainable media markets, both on- and off-line.

2.1. INTRODUCTION

Building information integrity and addressing disinformation rest in large part on the resilience of citizens, as well as on the actors that produce content and the channels via which it is distributed, namely online and social media platforms and traditional media. The share of the population that regularly receives news from traditional and local media sources has declined, as people have increasingly shifted to receiving news on social media platforms. A 2023 study of 16 countries from around the world – all of which scheduled to hold elections within the subsequent year – found that 56% of internet users frequently use social media as their primary source of news, surpassing television at 44% (Quétier-Parent, Lamotte and Gallard, 2023[1]).

Examples from specific countries show similar trends. For example, in the United Kingdom, the share of population that uses print media as its primary source of news has fallen from 59% in 2013 to 14% in 2023, while the share of the population that uses social media as its primary source has increased from 20% to 38%. In the same period, the use of social media as a prime media source increased from 27% to 48% in the United States, and from 18% to 29% in Germany (Newman et al., 2023[2]). While data on news consumption patterns is inherently difficult to collect and compare across countries, the broad trends, particularly within younger populations, consistently show a shift toward the use of social media as a primary source of news.

The trend away from traditional media is particularly clear at the local and regional levels and is widespread across OECD countries and beyond, reflecting the continued evolution in the move toward a digital, mobile, and platform-dominated media environment. These trends also suggest that younger generations, who have grown up with digital media, will likely continue to primarily engage with online platforms rather than legacy platforms for getting and sharing information (Newman et al., 2023[2]).

Today, both online and offline engagement is increasingly shaped by information flows on online platforms. The impact of online platforms goes beyond its use as a direct source of information, as feedback loops – where mis- and disinformation, including conspiracy theories, that spreads online is picked up by traditional media outlets – thereby further amplifying and giving credibility to the content (OECD, 2022[3]). Online platforms also offer novel and efficient avenues for amplifying foreign information manipulation and interference campaigns, which attempt to illegitimately shape public opinion and discourse, undermine trust in democracy, and increase polarisation, often in parallel with other foreign interference efforts.

Given the increasingly important role played by online platforms in the information space and the incentives for private companies' algorithms to amplify engaging (and often sensational or polarising) content, building the understanding of how these technologies can be misused to threaten basic elements of democratic life will be essential to inform effective policy responses. As it stands, limited understanding of how online and social media platforms function, of data flows within and across them, and of how they are being used, inhibits effective policy responses.

What is more, the reduced reach of, and trust in, traditional media combined with risks of market concentration and capture have further eroded access to quality content and information integrity in many countries. A plural and independent media sector plays an essential role in facilitating public discourse, and reinforcing democracy cannot be achieved without strengthening the role of quality and trusted news media sources.

For that reason, policy interventions to promote transparent and diverse media and information spaces can be grouped around:

- Identifying a range of efforts encouraging accountability and transparency of online and social media platforms,
- Promoting plural, independent, and competitive media and information markets, and
- Countering specific risks, such as foreign information manipulation and interference, elections and disinformation, and those posed by generative artificial intelligence.

2.2. ENCOURAGING ACCOUNTABILITY AND TRANSPARENCY OF ONLINE AND SOCIAL MEDIA PLATFORMS

Given the prominent role and impact that online and social media platforms have in the information space, the benefits of accountability and transparency in the way they are designed and operated are increasingly understood. The priority in this space should be to analyse how policies can call for accountability, build understanding of their business models and the related risks to democratic processes, mitigate harms, and promote healthier information spaces.

A prominent threat to information integrity in democratic systems is the use of digital platforms, including social media, by domestic and foreign actors to manipulate and disinform the public. To mitigate similar risks in traditional media, for example, news outlets have historically been subject to various regulatory frameworks. Such oversight is due to traditional media's role in creating, editing, and selecting content, as well as their use of limited public resources (e.g. broadcast spectrum). These policies often cover areas like standards, ownership restrictions, and licensing requirements, and complement strong self-regulatory practices of the profession.

Online platforms, however, do not claim editorial control over the user-generated content they host, making it a challenge to apply traditional media regulatory approaches. Social media platforms often enjoy specific legal protections as online intermediaries, shielding them from liability for user-generated content, for example via Section 230 of the 1996 Communications Decency Act in the United States.

Part of the challenges governments face in finding the right mix of approaches to protect information integrity owes to the global scope and reach of online platforms. Policies are typically implemented within jurisdictions whose size – even if encompassing multiple countries, as in the European Union – does not match the global scope and reach of online platforms. Such mismatch is a particular challenge when it comes to increasing platform transparency, since fragmented and inconsistent international obligations hinder the development of a comprehensive picture of data flows and information integrity risks, policies put in place to mitigate them, and the related results in the online information environment (Lai, Shiffman and Wanless, 2023[4]). Additionally, the role of private ownership of online platforms, which are effectively public spaces for news dissemination and debate often operating opaquely under their own terms of service and community guidelines, is important to bear in mind. Together, this context limits understanding of how information flows and, consequently, what policies work to mitigate the harms of disinformation.

To this end, governments can prioritise, as appropriate:

- Moving beyond self-regulation and clarifying the role and strategies of state-led policies, and
- Policy levers to encourage accountability and transparency.

2.2.1. Moving beyond self-regulation and clarifying the role and strategies of state-led policies

Self-regulation, which takes place when a group of firms or individuals exert control over their own membership and behaviour, has to date been the predominant approach taken in setting standards for online platforms. In information integrity, self-regulation refers to voluntary compliance to codes of conduct, guidelines, and other mechanisms to address issues like content moderation, privacy, or ethical practices. Such mechanisms are widely considered to benefit from the higher levels of relevant expertise and technical knowledge of the industry – in this case the platforms themselves – which in turn helps drive greater effectiveness and efficiency.

Notably, self-regulation can incorporate diverse arrangements, from completely private to varying degrees of government engagement, including around government involvement in developing or approving draft rules (Baldwin, Cave and Lodge, 2011[5]). Self-regulation allows for flexibility and industry-specific approaches; particularly for media and journalism organisations, this approach can play an important role in building capacity of news organisations to develop quality, factual content and prevent the inadvertent spread of misinformation. Self-regulatory mechanisms, such as press councils, can also play a critical role in monitoring the abuse of laws against journalists and advocating on their behalf (Lim and Bradshaw, 2023[6]).

For example, the Santa Clara Principles present a prominent self-regulatory effort focused on issues of information integrity and transparency that is not led by governments.[1] Adopted in 2018, these principles are a voluntary set of recommendations for companies that are designed to provide transparency and meaningful due process to impacted users of online platforms. The principles call for clarity of platforms' content moderation efforts; clear notice to affected users; and a robust appeals process. The Santa Clara Principles are designed to help guide, evaluate, and compare companies' practices and activities. Additionally, the Coalition for Content Provenance and Authenticity (C2PA) seeks to increase transparency of specific content. The C2PA was founded February 2021 by Microsoft and Adobe and included Arm, BBC, Intel, and Truepic; today, membership also includes Google, Sony, Meta, OpenAI, and several camera manufacturers, content creators, and non-governmental organisations. It addresses disinformation online by creating technical standards for certifying the source and history (or provenance) of specific content, to help verify who, how, when, and where it was created or edited, should the authors wish to include that information.[2]

In the Netherlands, the Ministry of the Interior and Kingdom Relations developed a Code of Conduct Transparency Online Political Advertisements in 2021 to prevent the spread of misleading information during elections, highlighting the potential involvement of the state in otherwise self-regulatory initiatives. The Code of Conduct is voluntary and open to all political parties and online platforms to help promote "transparency, privacy, security, fairness, and integrity of elections." Notably, participation is voluntary and the code of conduct notes that it does not replace other regulatory initiatives. While compliance is not enforceable, the code provides a signaling function of illustrating good conduct (at its launch, 11 out of 13 parliamentary parties and Facebook, Google, Snapchat, and TikTok had signed) (Government of the Netherlands, 2021[7]).

And yet, without democratic oversight or reporting requirements, self-regulatory regimes may generate questions of accountability. What is more, where self-regulation operates as a voluntary mechanism, the public may end up being ill-protected by regimes that effectively control the most responsible members of a field but leave unregulated those firms that are least inclined to serve the public or consumer interest (Baldwin, Cave and Lodge, 2011[5]).

X's announcement in May 2023 that it was withdrawing from its voluntary participation in the 2018 European Union Code of Practice on Disinformation[3] points to the limitations of voluntary codes of practice and principles (Lomas, 2023[8]). The Code was the first self-regulatory instrument to which leading industry actors, including Facebook, Google, Microsoft, Mozilla, TikTok, and Twitter (now X), voluntarily agreed. X's withdrawal was preceded by an announcement in February 2023 by the European Commission that the company's first baseline transparency report for the Code of Practice fell short of the expectations set by the other platforms in terms of the data it provided and information on commitments to work with fact checkers (European Commission, 2023[9]), further clarifying the challenge self-regulatory tools pose in enabling transparent, consistent, and comprehensive monitoring and reporting.

Mitigating the challenges of voluntary self-regulation, co-regulatory approaches incorporate industry expertise and self-governance and can allow for governments to take over oversight, enforcement, or ratification of self-regulation mechanisms (Baldwin, Cave and Lodge, 2011[5]). For example, the European Code of Practice was updated and revised in 2022, with the aim for it to become a co-regulatory instrument and serve as a strengthened monitoring framework under the Digital Services Act's (DSA) framework. The updated version of the Code contains 44 commitments and 128 specific measures covering issues around demonetisation and reducing financial incentives for spreaders of disinformation; increasing transparency of political advertising; reducing manipulative behaviour and fake accounts; supporting researcher access to platforms' data; among others.

In Australia, the Code of Practice on Disinformation and Misinformation was published in February 2021 by the Digital Industry Group Inc. (DIGI). While the code is voluntary and aims to provide safeguards against harms from the spread of false and misleading content on digital platforms, the Australian Communications and Media Authority (ACMA) oversees the Code of Practice and works with DIGI and the signatories to assess signatories' transparency reports, examine how signatories handle user complaints, and encourage more platforms to sign up to the code (see Box 2.1).

Box 2.1. Australia – Voluntary Code of Practice on Disinformation and Misinformation

Based on the Australian government's request in 2019 and learnings from the European Union's Code of Practice on Disinformation, the Digital Industry Group Inc (DIGI), a non-profit industry association, published the Australian Code of Practice on Disinformation and Misinformation in 2021. The aim of the code is to provide transparency about the safeguards digital platforms employ against harms from the spread of disinformation and misinformation.

The voluntary code currently has eight signatories: Adobe, Apple, Google, Meta, Microsoft, Redbubble, TikTok and Twitch. All signatories commit to:

- reducing the risk of harms arising from disinformation and misinformation; and
- publishing an annual transparency report about the steps they are taking to combat misinformation and disinformation.

Depending on the nature of their service, signatories may also commit to providing information about their efforts to:

- disrupting advertising and monetisation incentives for the spread of mis- and disinformation
- working to ensure the security and integrity of the platform's services and products
- empowering users to make better-informed choices of digital content and helping them identify false and misleading content
- increasing transparency around political advertising
- supporting research that improves public understanding of mis- and disinformation.

DIGI is the administrator of the Code. In October 2021, DIGI strengthened the code by instituting a governance framework and establishing a complaints facility for the public to report breaches by signatories of their commitments. In December 2022, DIGI published an updated version of the Code. Updates focused on making it easier for smaller companies to adopt the Code and clarifying the specific products and services covered.

While the ACMA currently has no formal regulatory role in relation to disinformation and misinformation, it oversees the operation of the Code, which includes reporting on digital platforms' disinformation and news quality measures and engaging consistently with DIGI, signatories and other parties on the operation of, and potential improvements to, the Code, and encourages more platforms to join.

Source: Government of Australia (2024[10]), "Online misinformation", Australian Communications and Media Authority, https ://www.acma.gov.au/online-misinformation.

The limitations posed by existing self- and co-regulatory regimes increase the risk that they will not sufficiently mitigate the threats posed by those actors that do the most to undermine information integrity in democracies, as well as by those who merely do not wish to engage. Such risks point to the importance of government involvement in designing, enforcing, and updating regulatory responses, where relevant and appropriate. While designing policies that protect and promote freedom of expression and active, well-informed democratic debate require engagement with civil society and private sector actors, responses cannot be left to them alone. This said, these self-regulatory efforts have had value over the years in fostering dialogue between governments and platforms on the issues at stake and helping to identify the various policy options at hand. These experiences provide an important basis on which to build.

2.2.2. Policy levers to encourage accountability and transparency

As noted in the introduction, given risks to freedom of expression that content-specific policies raise, responses should largely focus on clarifying the responsibilities online platforms have regarding their role as essential actors in the information space. In this respect, governments should ensure a clear and predictable legal framework, where the rules are clear to avoid incentivising privatised censorship (Council of Europe, 2021[11]).

Furthermore, the largely opaque operations of major tech companies prevent understanding of the role of online platforms in shaping the information environment and the actions they have taken to mitigate harmful behaviours (Lai, Shiffman and Wanless, 2023[4]). Strategies focused on increasing transparency can help build understanding around how online platforms operate and can help ensure that online platforms' rules and implementation are clear, predictable, and proportionate. Because of the information asymmetry between online platforms and governments about how content is spread and what interventions work, transparency is also an important tool in helping governments and independent researchers better understand the information space, which in turn will help monitor the impact and effectiveness of responses and inform policymaking (OECD, 2022[3]). This opportunity speaks to the broader need to enhance measurement capabilities of relevant policy actions in this space.

Online platforms do not generally have an incentive to share information with researchers, regulators, or the public on policies, processes, algorithms, or content flows primarily due to cost, privacy, and competition concerns. By making information more accessible and accurate, policies may help ensure information is provided to facilitate better understanding of the information space and the actors therein and allow for independent verification of platform claims. Risks in other industries provide meaningful examples in this respect: until governments required its disclosure, accurate information was unavailable to the public in markets as diverse as the nicotine content of cigarettes, fuel economy for cars, or food safety (Baldwin, Cave and Lodge, 2011[5]).

Several laws have recently been implemented or discussed that focus on a wide range of transparency issues. The European Union's Digital Services Act (DSA), the UK Online Safety Act, as well as draft U.S. legislation, such as the Digital Services Oversight and Safety Act, and the Platform Accountability and Consumer Transparency Act, all reflect growing demands for greater platform transparency (Lai, Shiffman and Wanless, 2023[4]). Government regulation to promote transparency and accountability can also build on existing or similar self-regulatory efforts, as seen in the European Union, where the voluntary Code of Practice on Disinformation is now embedded in the DSA.

Greater transparency is only part of the solution for the problem of information manipulation on social platforms. Artificial amplification of content, for example via social media bots disguised as human users, can distort conversations online by boosting the apparent popularity of certain messages and accounts. This artificial amplification can be particularly harmful during elections, natural disasters, or other crisis situations.

Governments are increasingly identifying policy responses to improve the authenticity of the information space online. For example, in 2018, California introduced the Bolstering Online Transparency Act (BOT Act), which prohibits online bots from hiding their identities to appear as a human user (State of California, 2018[12]). In 2023, the Lithuanian Parliament began discussions regarding amendments to the Law on Public Information and the Criminal Code, which could give Lithuanian government the right to order social platforms and other information providers to "remove artificially increased numbers of page views, comments, shares, likes, followers, and/or subscribers of content within eight hours, or to withdraw the possibility of access to this content." The discussions also included the potential for criminal sanctions and imprisonment for the artificial dissemination of content on platforms.[4]

Across policy responses, consideration should be given to their potential impact on competition. Larger online platforms are better equipped to navigate more onerous liability and transparency rules (such as through buying or developing filtering technologies and complying with deadlines for removing and reporting on content) (Council of Europe, 2021[11]). Specifically, it may be useful to vary the extent and

burden of mandated transparency relative to a platform's size, so that compliance does not become a barrier to entry. For example, the DSA imposes additional requirements for Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) related to identifying and auditing systemic risk, enhanced transparency reporting on content moderation, advertising transparency, and access to data about content shared on the platforms (European Union, 2022[13]).

Ultimately, it is important to outline the specific objectives, values, and aims that increased transparency requirements are seeking to achieve, as there are several trade-offs and considerations that governments should bear in mind. Regulations in this space, where relevant, should be guided by proportionality, as designing and delivering regulations in a proportional way is an essential approach to improving efficiency, strengthening effectiveness, and avoiding unnecessary administrative burden (OECD, 2021[14]). Policy responses focused on platforms should be used as a mechanism by which governments – and the public more widely – can better comprehend and respond to the behaviours and business models of key actors whose technology dominates that space, understand and mitigate specific risks, and build knowledge of the information environment more widely.

To that end, policies encouraging accountability and transparency for online platforms and services may apply to a wide range of topics, including:

- the role of online intermediary liability protection in balancing platforms' roles and responsibilities,
- transparency around moderation policies and policy development, risk assessment and management processes, and algorithms, to provide valuable comparative information on how online platforms operate, and
- Increased transparency of online platform behaviour and content data to build understanding of the information space.

Online intermediary liability regimes should clarify platforms' roles and responsibilities

A key regulation in the information space concerns online intermediary liability, which establishes the legal responsibility or accountability of intermediaries, such as internet service providers or social media platforms, for the content shared or created by their users. The growing importance of online intermediaries in how people get and share information has heightened the emphasis on defining their legal liability for harms caused by content shared by – or activities carried out by – users of intermediaries' services (Shmon and Pederson, 2022[15]).

Broadly, online intermediary liability regimes attempt to balance the extent to which platforms are held liable for content shared on their platforms with the need to support freedom of expression, innovation, and promoting an online environment conducive to democratic engagement (Shmon and Pederson, 2022[16]). Intermediary liability regimes, and the "safe harbour" they provide to liability for user-generated content, range in scope. These laws generally try to weigh three goals: 1) enabling platforms to take content moderation actions (indeed, platforms typically have greater obligations and fewer legal protections for content that poses the greatest threats or that is otherwise illegal); 2) protecting speech and public participation by reducing platforms' incentives to over-enforce or restrict users' lawful speech unnecessarily; and 3) encouraging innovation and economic growth by providing space for market entrants to develop and build platforms by shielding them from being exposed to overly burdensome moderation requirements or legal risk (Keller, 2019[17]). Related to the information space, intermediary liability laws are particularly relevant for enabling platforms to pursue content moderation decisions for content that is not otherwise illegal, while reducing the incentive for imposing undue restrictions on speech.

Section 230 of the United States Communications Decency Act of 1996 is an example of an immunity-based approach. This clause has widely been seen to be instrumental in fostering innovation and growth of the internet and online platforms (OECD, 2011[18]). Section 230 provides immunity from liability to providers and users of an "interactive computer service" that publish information provided by users of the platforms. This protection has empowered online services to develop and maintain open platforms that facilitate free expression (OECD, 2011[18]). Section 230 also, importantly, removes liability for platform decisions regarding moderation, filtering, and amplification of user-generated content, enabling platforms to moderate and disseminate content largely as they see fit (see Box 2.2 for the specific language).

Box 2.2. Relevant language from Section 230 of the United States Communications Decency Act (1996)

(1) "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) No provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."

(Per the law, "the term 'information content provider' means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.")

Section 230 does not, however, extend to immunity violations of federal criminal law, intellectual property law or electronic communications privacy law.

Source: For more information, see Communications Decency Act, 47 U.S.C. § 230 (1996).

The immunity approach has also, however, led to criticisms regarding lack of accountability of online platforms (or "duty-of-care") for the content they host. The aim of this approach, as seen, for example, in the UK Online Safety Act of 2023, is for online platforms to take measures to assess risks, as well as prevent and mitigate reasonably foreseeable harmful and illegal content. Beyond broad immunity, there are three common, and not mutually exclusive, approaches to narrowing intermediary liability. For example, the awareness or "actual knowledge" approach holds websites and online platforms accountable only for content of which they are aware or have "actual knowledge". Japan's Provider Liability Limitation Act, enacted in 2001, falls into this category. A second approach is the "notice and takedown" approach, which requires online services to comply with judicial requests. The 2014 Brazilian Marco Civil da Internet, for example, provides general liability exemption for content generated by third parties, with exceptions for copyright, unauthorised disclosure of private images containing nudity and/or sexual activities, and obligations to comply with judicial decisions ordering content removal.[5] Furthermore, New Zealand's Harmful Digital Communications Act 2015 provides liability exemption if websites comply with notice of complaint processes.

The scale of content shared online will continue to make private platforms powerful actors in determining what is seen and shared; privately owned platforms will by necessity continue to serve as moderators for conversation and debate among citizens (Douek, 2021[19]). To that end, intermediary liability protections should be designed in a way that fosters a free and open internet while enabling platform responsibility to address legitimate concerns around false, misleading, and otherwise harmful or illegal content.

Increasing transparency and understanding of how online platforms are designed and function

Broadly, disclosure requirements allow consumers to make decisions on their acceptability of the processes employed in producing products or services (Baldwin, Cave and Lodge, 2011[5]). One avenue for mandating transparency therefore includes a focus on the policies, policy development, processes, and algorithms employed by online platforms. Requiring platforms to disclose information on terms of service and privacy policies; disclosure on use of behavioural data and user data shared with third parties; procedures, guidelines, and tools that inform the content moderation and algorithmic decision making; and processes of complaint handling can empower users to better understand data handling practices and rule enforcement. Disclosures can play a useful role in safeguarding users' rights and promoting accountability by platforms, as public scrutiny can highlight potential biases or unfair practices. Clarifying these processes may also reduce concerns of those companies that advertise on online platforms of reputational risks to

being associated with the spread of disinformation, facilitating a market-based inducement to healthier online information spaces.

The goal of policies in this space is to "institutionalise, incentivise, and verify" the rules and systems that platforms and other relevant actors put in place to oversee the information spaces they control (Douek, 2021[19]). These transparency requirements are particularly important given the rapid evolution of platform practices and policies, as they allow regulators and the public to verify the effectiveness of the rules and content moderation systems online platforms have put in place. Such oversight can also help identify blind spots in company processes (Douek, 2021[19]).

For example, individuals are often unaware of how their online statements, content, and behaviour are turned into data and how algorithms used by online platforms sort content to profile and target them through advertising (OECD, 2022[20]). Efforts to increase transparency of privacy policies of online platforms can provide users with valuable information on how their personal data is used.

These discussions, however, cannot be separated from broader privacy debates across democracies. Specifically, privacy regulations can limit the unchecked gathering of personal information, making it harder for malicious or other actors to manipulate or influence individuals through targeted content. By limiting access to the information that enables personalised targeting and polarising messages, data privacy laws can potentially help prevent unwanted message targeting (Campbell, 2019[21]). The GDPR (General Data Protection Regulation) in the European Union, for example, provides a wide range of legal provisions designed to safeguard individuals' personal data and privacy rights, including that organisations that collect, process, or store personal information obtain explicit consent for data processing, provide transparent privacy policies, and ensure appropriate security measures. Additionally, these laws grant individuals greater control over their data, including the right to access, correct, or erase their information, as well as the right to know how their data is being used (European Council, 2022[22]). By safeguarding individuals' personal data and enforcing data handling practices, privacy laws can create a more transparent and accountable environment online.

Transparency requirements may also increase information sharing on platform architecture and algorithms. There is a limited public understanding of how the algorithms that drive information curation, amplification, and engagement on platforms are developed and deployed. These algorithms, in turn, have faced criticism for helping to drive radicalisation of users and promoting and amplifying harmful content. To address these concerns, transparency requirements can enable greater understanding of the kinds of algorithms used by online platforms and provide insight into their impacts and consequences (Lai, Shiffman and Wanless, 2023[4]).

Legislation could enable researchers and regulators (as the DSA does in the EU market) to have greater insight into the algorithms used in content moderation, prioritisation, advertising, and recommendation, as well as how these algorithms affect the spread of content on the platforms. These insights would allow for external and independent assessment to better inform policymakers and the public of information integrity risks and help guide policies to mitigate them (MacCarthy, 2021[23]).

Facilitating the standardisation of the information provided regarding how online services formulate, communicate, and enforce their rules can encourage the creation of best practices for public policy development and inform ways to measure the impact of those interventions (Lai, Shiffman and Wanless, 2023[4]). The DSA includes requirements for the publication of transparency reports and more information about content moderation and terms of service. The Australian Government's draft Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill[6] proposes new powers for the independent regulator, the Australian Communications and Media Authority's (ACMA), which aim to address harmful misinformation and disinformation online, while upholding the right to freedom of expression that is fundamental to democracy. The proposed powers are consistent with the key recommendations in the ACMA's June 2021 *Report to government on the adequacy of digital platforms' disinformation and news quality measures*. One of the key elements proposed in the report is a focus on enabling the ACMA to gather information from digital platform providers on their systems and processes to combat harmful online misinformation and disinformation (see Box 2.3).

Box 2.3. Overview of Australia's Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill

On 20 January 2023, the Australian Government announced its intention to introduce new legislation granting ACMA proposed new powers to combat harmful online misinformation and disinformation.

On 25 June 2023, the Australian Government released an exposure draft of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill for public consultation, which closed on 20 August 2023. The Bill focuses on improving digital platforms' transparency around how they handle and manage misinformation and disinformation on their services. The draft Bill builds on the existing voluntary Australian Code of Practice on Disinformation and Misinformation that major digital platforms have already signed up to.

The main objectives of the draft Bill are to provide new functions to ACMA to encourage, and if needed require, online platforms to take steps to counter the threat posed by the spread of misinformation and disinformation. The draft Bill proposes new powers for the ACMA, including record-keeping, information gathering, and would reserve code- and standard-making powers. The powers would:

- enable the ACMA to gather information from digital platform providers, or require them to keep certain records about matters regarding misinformation and disinformation
- enable the ACMA to request and assist industry to develop a code of practice covering measures to combat misinformation and disinformation on digital platforms, which the ACMA could register and enforce
- allow the ACMA to create and enforce an industry standard (a stronger form of regulation), should a code of practice be deemed ineffective in combatting misinformation and disinformation on digital platforms.

The draft Bill also includes a number of safeguards to protect freedom of speech and public debate and the framework would be open to regular system reviews and parliamentary oversight.

Source: Australian Competition and Consumer Commission (2019[24]), *Digital Platforms Inquiry Final Report*, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf; Australian Government (2023[25]), *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023—guidance note*, https://www.infrastructure.gov.au/department/media/publications/communications-legislation-amendment-combatting-misinformation-and-disinformation-bill-2023-guidance.

Increasing transparency of information flows and content on online platforms

Beyond process and policy transparency, countries have used policies around the sharing of metadata with external researchers to build general understanding around disinformation flows and how platforms moderate or remove (or not) types of content. Data transparency requirements for online platforms can provide valuable insights and context about user interactions and behaviours, information flows within and across platforms, and patterns of engagement, all of which can facilitate the development of a robust evidence-base for measurement moving forward.

Increasing access to behaviour and content data to build societal understanding of the information space online

Increased clarity and consistency of information provided could help build a better understanding around what data is most helpful when designing and measuring the impact of interventions. These transparency efforts may also continue to identify specifically how such data can be provided and analysed in a way that respects privacy and competition concerns and clearly outlines which actors have access to data (Lai, Shiffman and Wanless, 2023[4]). Given the importance of online platforms in the information space, facilitating greater transparency about how content is spread across their platforms will likely be a necessary component to better understand the information space. Finally, increasing the visibility into actions of online platforms and the way content flows may help provide an incentive for them to clarify and improve content moderation policies and actions (MacCarthy, 2021[23]).

One category of relevant data includes user-level information to provide general insights into who the users of platforms are and how they engage on the platform. Reporting may include aggregated information about types of users (using age groups, gender, and location data). It may also include types of content of public posts, comments, and engagement. Such public data (not including private posts or messages) that does not include personally identifiable information could provide a helpful baseline of what groups are most active and common types of online behaviour to help identify patterns and changes over time (Lai, Shiffman and Wanless, 2023[4]).

Enabling independent researchers to verify and confirm platforms' public disclosures could be a useful model to help hold services accountable. Mandating that steps are taken to ensure research is conducted for legitimate aims and that researchers implement privacy and security protections for datasets used will be important guardrails to prevent abuse (Goldman, 2022[26]) (Forum on Information and Democracy, 2020[27]). Transparency requirements do not necessarily mean the information will be made public; indeed, the level of detail required can and probably should differ across audiences, given the risk that potentially sensitive content may be misused if made available to the public (Lai, Shiffman and Wanless, 2023[4]).

For example, Article 40 of the Digital Services Act (DSA) gives digital regulators within each EU member states the ability to mandate that platforms share data with researchers under clearly outlined processes (see Box 2.4).[7] While questions remain around compliance, including whether researcher access programmes can be extended to other countries and how to handle data of residents outside of Europe, the DSA puts into practice many of the aims of this category of transparency regulation (Lenhart, 2023[28]).

Box 2.4. DSA Article 40 – Data access and scrutiny

Article 40 of the DSA is designed to promote transparency of data held by online platforms and to facilitate public interest research that will build understanding of how online platforms work. Specifically, it provides the process by which "vetted researchers" can apply for specific public data accessible on online interfaces to "conduct research that contributes to the detection, identification and understanding of systemic risks." The DSA also notes that very large online platforms and very large online search engines shall be required to respond to data access requests, and provide the data to the researchers unless providing access to the data "will lead to significant vulnerabilities in the security of their service or the protection of confidential information…and trade secrets."

Notably, the DSA also establishes 'vetted researchers', who are given the ability to apply for specific data requests. Digital services co-ordinators, who will co-ordinate and oversea the application of the DSA, will grant this status to researchers who:

- demonstrate that they are affiliated to a recognised research organisation
- demonstrate that they are independent from commercial interests
- disclose the funding of the research
- demonstrate that they can fulfil the specific data security and confidentiality requirements, that they can protect personal data, and that they describe in their request the appropriate technical and organisational measures that they have put in place
- demonstrate that their requests are proportionate to the purposes of their research, and that the expected results of that research will contribute to the public interest
- commit to making their research results publicly available free of charge, within a reasonable period after the completion of the research.

Source: European Union (2022[13]), Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?ur.

Reporting requirements could also include greater transparency around requests from third parties, such as researchers and data brokerage firms, for access to data. As it stands, there is a limited understanding of who has access to user data and how that data is used. Governments could therefore require additional reporting by platforms on data sharing with third parties, including on whom platforms sell data to, who they buy data from (such as data brokers), and information on the relationships that platforms have with other actors who handle, buy, request, or have access to user data (Lai, Shiffman and Wanless, 2023[4]). Illuminating these relationships could be a useful mechanism to track data flows and better understand who has access to what kinds of information. To that end, privacy laws may be helpful in clarifying what personal data is considered public while also clarifying the acceptable use of data for research (Lenhart, 2023[28]).

Researchers would also benefit from greater harmonisation and facilitation of data access. Removing barriers to access could reduce costs and allow more informative analysis across multiple social media networks and countries. Facilitating cross-border research, for example clarifying areas of potential legal conflict and exploring compromise on data sharing or safe harbours that allow cross-border access to data for researchers, will be particularly useful to develop a cross-border understanding of the information space (Lenhart, 2023[28]). This again would require upholding privacy rights, securing proprietary corporate information, and avoiding capture by commercial and government interests, though the aim of data collaboration could facilitate a more harmonised approach to building resilience and improving information integrity (Scott, 2023[29]).

Increasing transparency of political advertisements on online platforms

Policies may also seek to increase transparency around political advertisements on platforms. Political advertisements are defined as those that are made by or on behalf of a candidate or party, that communicate a message relating to a political matter of national or local importance, or are likely to influence the outcome of an election.[8] The data could include increasing information around provenance of the content (for example, while campaigns and political organisations may be required to report how they spend money on advertisements, the same may not be true for how advertising agencies and consultancies spend money on their behalf, which some research suggests could make up the vast majority of the spending); increasing the detail provided and standardising reporting; and storage and research access to reduce the variation in the data and access provided by existing platform ad libraries (Brennen and Perault, 2021[30]). Increasing information around political advertisers' actions on platforms may also be gathered from reporting requirements on a user's advertising activity. Reporting could include details on the audiences targeted as well as the content of the advertisements. This data could increase understanding around the advertisers' influence targets, at least regarding broad groups of users (Lai, Shiffman and Wanless, 2023[4]).

Several efforts have been made in this direction, including the 2019 decision of Israel's Central Elections Committee, which banned anonymous election ads on all platforms, including social media, from both within Israel and abroad. In effect, the ruling applied the restrictions in the Elections Law (Propaganda Methods) of 1959, which primarily deals with advertising on billboards, radio, TV, regional radio stations, and published election surveys, to advertising on the internet (The Times of Israel, 2019[31]). Most recently, in Europe, the DSA required that platforms provide "information necessary for users to understand when and on whose behalf the advertisement is presented".

Another component of political advertising policy could consider requiring the creation and maintenance of political advertisement databases that are standardised, publicly accessible, and searchable (Brennen and Perault, 2021[30]). In addition to the content of the advertisements, the source of the advertisement and money behind it, as well as targeting data and profiling used, could be included. Such a public repository would be valuable to researchers, advocates, and regulators to better understand the flow of information around elections and policy debates, as well as help inform future regulatory actions, as appropriate (MacCarthy, 2021[23]). Along these lines, the DSA will require Very Large Online Platforms and Very large Online Search Engines to "ensure public access to repositories of advertisements presented on their online interfaces to facilitate supervision and research into emerging risks brought about by the distribution of advertising online

[…] Repositories should include the content of advertisements […] and related data on the advertiser, and, if different, the natural or legal person who paid for the advertisement, and the delivery of the advertisement, in particular where targeted advertising is concerned (European Union, 2022[13])."

2.3. PROMOTING PLURALISTIC, INDEPENDENT, AND COMPETITIVE MEDIA AND INFORMATION MARKETS

A diverse and independent media sector, and an information ecosystem that supports journalism and facilitates the creation of high-quality news creation, play an essential role in enabling open and democratic societies by providing reliable information, bringing issues to the public agenda, facilitating debate, serving as a watchdog for the public interest, and holding public actors accountable (OECD, 2014[32]). Reduced access to and trust in providers of accurate and verifiable information prevents citizens from accessing shared facts, inhibits informed decision-making and democratic debate, and opens the door for further amplification for the spread of mis- and disinformation.

The 2023 World Press Freedom Index – which evaluates the environment for journalism in 180 countries and territories – reveals that the proportion of OECD countries where the environment is "good" for journalism has more than halved over eight years. While 49% of OECD countries were ranked as "good" in the 2015 World Press Freedom Index, this fell to 21% in 2023. Globally, the share fell from 21% to 4%, which emphasises the relative strength of OECD members (RSF, 2023[33]). Trust data also highlight the challenging dynamics facing traditional media. Notably, only four out of ten (38.8%) respondents to the 2021 OECD Survey on Drivers of Trust in Public Institutions reported trusting the news media (OECD, 2022[34]), and other research found that trust in the news continued to fall globally between 2022-2023 (Newman et al., 2023[2]).

These dynamics are taking place in a context of ongoing threats to the safety of journalists. Estimates of journalists killed worldwide between 2010 and 2020 range from 937 (RSF, 2020[35]) to 956 (UNESCO, 2021[36]). Beyond constituting illegal acts, physical harms, and human rights violations, attacks against journalists limit free expression and deprive others of their rights to receive information, thus hampering freedom of expression, limiting civic space, and reducing the ability for informed public debate (OECD, 2022[20]). In addition to the ensuring freedom of expression, governments must protect journalists, media workers, and researchers, and monitor, investigate, and provide access to justice for threats and attacks against them. This is the aim, notably, of the 2016 Council of Europe Recommendation on the protection of journalism and safety of journalists and other media actors (Council of Europe, 2016[37]). Along a similar line, the Council of Europe Safety of Journalists Platform[9] and the EU Media Freedom Rapid Response (MFRR) Monitor[10] report on serious threats to the safety of journalists and media freedom, while the Council of Europe Journalists Matter is a campaign that seeks to promote press freedom and protect journalists from violence, threats, and harassment while performing their duties.[11]

Traditional media have also faced financial problems due to dwindling advertising revenue, as the advertising market shifted to digital especially to online platforms. In the United States, for example, newspaper publishers in 2020 earned less than half of what they earned in 2002 (United States Department of Justice, 2022[38]). The Australian Competition and Consumer Commission (ACCC) found that the number of journalists in traditional print media businesses fell by 20% from 2014 to 2018 (Australian Competition and Consumer Commission, 2019[24]). Smaller regional media outlets are often particularly hard hit. In the United Kingdom, the regional newspaper advertising market was worth GBP 2.5 billion in the 1990s; at the end of 2022, it was valued at GBP 241 million (Sweney, 2023[39]). Increasing digital subscription are compensating only a minor part of the former incomes.

The decline of small regional media often leaves entire regions without quality local media. The United States has lost almost 2 900 newspapers since 2005 (now leaving only 6 000 newspapers in the country), many of which were the sole provider of local news in small and mid-sized communities. In addition, the country has lost almost two-thirds of its newspaper journalists – 43 000 – in that same period (Medill Local News Initiative, 2023[40]). The Australian government found that there had been a significant reduction in the number of articles published covering local government and local court issues in the 15 years to 2019, which is concerning given the important role such coverage plays in

exposing corruption and in holding governments, corporations, and individuals to account (Australian Competition and Consumer Commission, 2019[24]). The "media deserts" created by shortages in local media can lead to vacuums in the information environment that are often filled by news from online platforms and social media, further amplifying the opportunities for mis- and disinformation to spread. Evidence from Germany also shows that the decline of local media outlets has a negative impact on political polarisation (Ellger et al., 2021[41]).

In addition to the focus on online platforms' role in the information space, the structure of traditional media markets remains an essential public policy issue to help ensure the public has the information necessary for effective democratic engagement. Media capture, market concentration, and threats to local and community media can hamper broad public debate and promote one-sided views that can undermine information integrity (OECD, 2022[20]). Government policies can therefore play a constructive role in supporting democratic discourse through the promotion of media freedom, diversity, and independence. While these interventions are not specifically directed at countering disinformation, they nonetheless point to how governments can prioritise shifting media markets to help them serve as a necessary source of information within democracies.

The challenges facing media throughout democracies are a particular concern given the role the sector plays in supporting an informed citizenry, a well-functioning democracy, good governance, and reduced corruption. To that end, government responses designed to strengthen the traditional media sector include:

- Protecting and enhancing journalist safety
- Enhancing transparency and political independence of traditional media, and
- Preventing media capture and supporting a pluralistic and independent media environment

2.3.1. Information integrity requires a focus on journalist safety, transparency, and preventing media capture

Ensuring freedom of opinion and expression requires uncensored and unhindered access to the press and other media. To that end, establishing mechanisms to protect journalists and systematically investigating, monitoring, and providing access to justice for threats and attacks are also essential to ensuring journalists have the freedom to participate fully in the democratic process (OECD, 2022[20]). For example, the modified Luxembourg Criminal Code (*Loi du 7 août 2023 portant modification du Code pénal*) includes new penalties for attacks against journalists during demonstrations. In addition, persons who threaten individuals can be subject to imprisonment, with an aggravating factor if the target is a journalist. The code also specifies that the disclosure of private and professional information ('doxxing') can lead to criminal liability for the perpetrator, with again an aggravating factor if the target is a journalist (Grand Duchy of Luxembourg, 2023[42]).

Beyond a focus specifically on journalists, a related avenue to help prevent interference is to mitigate media capture and promote editorial independence. Media capture refers to situations where individuals or groups exert significant control over media organisations in a way that influences content and coverage. In these contexts, the media's ability to serve its democratic role as a "watchdog" is compromised (Nelson, 2017[43]). The risk of capture of a media outlet by political or private interests increases as the sector becomes more concentrated (Government of France, 2022[44]), where media ownership is consolidated in the hands of a few entities or individuals. These owners can in turn promote one-sided views that can lead to polarisation and impede balanced and diverse democratic debate (OECD, 2022[20]).

Policies can play a role first in maintaining a diverse and pluralistic market for traditional media by limiting market concentration in the sector. For example, policies can take the form of control on cross-media ownership (i.e. controls on joint ownership of broadcast channels in the same geographic region). Indeed, laws designed to prevent concentration proactively often form the main pillar of a state's efforts to guarantee media diversity and prevent concentration of opinion in the media sector (European Audiovisual Observatory, 2016[45]) (Nelson, 2017[43]). Notably, the EU Media Pluralism Monitor[12] is a tool that measures the state of media pluralism across 34 countries and makes recommendations for policy action.

Promoting diversity of media ownership through anti-trust and fair competition rules involves a range of considerations. A report by the French government

recommended assessing the impact of transactions on pluralism on a case-by-case basis, using an analysis based on qualitative indicators (promoting diversity of content, independence of information) and quantitative indicators (audience, coverage, economic viability of the operators) (Government of France, 2022[44]). This approach is similar to that taken in the United Kingdom. The 2003 Communications Act outlines public interest considerations for broadcasting and cross-media mergers, including that there be a "sufficient plurality of persons with control of the media enterprises"; that there be a wide range of broadcasting available that is both high quality and calculated to appeal to a wide variety of tastes and interests; and for media to have a genuine commitment to the accuracy and impartiality standards laid out elsewhere in the statute (Government of the UK, 2003[46]). Norway introduced an obligation for media enterprises and owners to provide information about ownership interests to the Norwegian Media Authority in order to create greater transparency, awareness, and knowledge of ownership interests in Norwegian media (Government of Norway, 2016[47]).

Second, policies that reinforce transparency in countries' media markets can play an important role in ensuring media independence from political and commercial interests and freedom from foreign or domestic political influence. Opaque ownership makes it difficult to identify underlying bias, potentially further undermining trust in the news media. Transparency is therefore a necessary – but not sufficient – policy response to reinforcing media plurality and increasing trust in the media sector (Craufurd Smith, Klimkiewicz and Ostling, 2021[48]).

Notably, the European Court of Human Rights has recognised a positive obligation on States that are parties to the European Convention on Human Rights to "put in place an appropriate legislative and administrative framework to guarantee effective [media] pluralism" and that such plurality cannot be fully effective without clear information. To that end, it recognised the value of media transparency and independence to democracy, specifically in the interests of individuals in having access to information "on all matters of public interest" and the ability of the media to perform their "vital role of 'public watchdog'" (European Court of Human Rights, 2001[49]). In addition, the 2018 Council of Europe Recommendation on media pluralism and transparency of media ownership notes that media freedom and pluralism are "crucial corollaries of the right to freedom of expression…and… are central to the functioning of a democratic society as they help to ensure the availability and accessibility of diverse information and views, on the basis of which individuals can form and express their opinions and exchange information and ideas" (Council of Europe, 2018[50]).

Requirements include transparency around media ownership, for example, by mandating full disclosure of owners, the size of the shareholdings, and their other economic and political interests. Ownership should refer to the "beneficial owner," or the "natural person(s) who ultimately owns[…]and/or exercises ultimate effective control (FATF, 2023[51])." The information provided should also "identify the natural person(s) who are the beneficial owner(s), and the means and mechanisms through ownership, control or other means (FATF, 2023[51])." Such information can provide policymakers, regulators, and the public with the relevant data needed to develop, monitor, and enforce ownership limits and prevent capture (Craufurd Smith, Klimkiewicz and Ostling, 2021[48]). More can be done in this space. In Europe, for example, while most countries (24 of 31)[13] require the disclosure of ownership information to public bodies, a minority (14 of 31) require disclosure to the public (Craufurd Smith, Klimkiewicz and Ostling, 2021[48]). In addition to beneficial ownership, information should also cover details of financial and other relations that could result in editorial influence and conflicts of interest, such as ownership in other industries with significant government interests, the holding of political office, and ensuring that government advertising budgets are allocated in an open and competitive way and independent of political influence (Nelson, 2017[43]).

Third, governments may also take clear positions on enforcing editorial independence. For example, Norway's Media Liability Act seeks "to facilitate open and informed public debate by ensuring editorial independence" by mandating that publishers appoint an independent editor. Specifically, this means that the owner or company management "cannot instruct or overrule the editor on editorial issues, nor can they demand to have access to…material before it is made available to the public."[14]

For its part, the proposed European Media Freedom Act seeks to protect media independence by strengthening

safeguards against political interference in editorial decisions, as well as promoting transparency of media ownership and of the allocation of state advertising. It also seeks to defend media pluralism by promoting the stable funding of public service media and requiring member states to assess the impact of media market concentrations on media pluralism and editorial independence and to create a new independent European Board for Media Services, comprised of national media authorities. Importantly, it also includes safeguards against the unjustified removal of media content produced according to professional standards. This "media privilege" considers membership of press councils as one of the benchmarks for identifying reliable news media, and broadly seeks to promote media and journalism's role in democratic discourse (European Commission, 2022[52]).

2.3.2. Governments can play an important role in supporting a diverse and independent media environment

Quality journalism is important for democracy and states should put in place effective policies to support it (Council of Europe, 2023[53]). Quality journalism, in particular quality investigative journalism, requires important financial resources. Governments can play an important role in supporting the survival and transformation of the media sector by providing various means of financial support, with safeguards around government influence on content.[15] At the national level, funding can take the form of support for independent public service broadcasters; direct subsidies and competitive or selective funds for private or non-profit media; and indirect measures such as tax subsidies. Governments may also provide Official Development Assistance (ODA) as a part of their efforts to support and develop diverse and independent journalism in aid-recipient countries (Forum on Information and Democracy, 2021[54]).

National-level support mechanisms

Independent public service broadcasters, which are partly or fully funded by public funds but are nevertheless editorially independent,[16] can play an instrumental role in strengthening information integrity, as they are seen as important sources of news in most OECD countries. Many public broadcasters also have a fact-checking function that enables them to play a direct role in countering disinformation. Examples include "*Vrai ou Faux*" by Franceinfo, a joint initiative by two French broadcasters, Radio France and France Télévision, as well fact-checking branches at Deutsche Welle and in the Lithuanian and Estonian public broadcasters. The Australian Broadcasting Corporation (ABC) also partners with Royal Melbourne Institute of Technology (RMIT) on "RMIT ABC Fact Check" to determine the accuracy of claims by politicians, public figures, advocacy groups, and institutions engaged in the public debate.

Direct and indirect financial support from governments may also go toward private media outlets that meet specific audience or other criteria, often in the form special taxation regimes and discounts on postage fees. Direct government support and indirect measures such as tax incentives remain important tools in supporting news media, provided they are transparent, objective and predictable (Council of Europe, 2023[53]). These policies have a historical legacy – in the United States, the Postal Service Act of 1792 provided postal subsidies as an indirect way of using public funds to support the economics of local newspapers (Medill Local News Initiative, 2023[40]). Within Europe, such indirect subsidies are the most common form of state subsidy, with 19 of 24 countries in a recent study having put in place transparent rules to allocate indirect subsidies. Such subsidies are widely considered less risky than more direct interventions given that indirect subsidies are harder to distribute in a selective way (Bleyer-Simon and Nenadić, 2021[55]). For example, in Norway, media organisations receive a value-added tax exemption (25%), not including certain electronic news services. Research has found that in high-income countries, indirect subsidies such as VAT exemptions for private print media and newspapers match and sometimes outweigh direct subsidies to public service media (Forum on Information and Democracy, 2021[54]).

Governments may also provide direct financial support, including for cultural, minority language media or for investigative journalism, fact checking projects, or for broader support and capacity building for traditional (particularly local and regional) media. Belgium created the *Fonds pour le journalisme* in 2009, which provides funding directly journalists and is managed independently by the Belgian Association of Professional Journalists. Additionally, the Luxembourg Law of 30 July 2021 ties the amount of aid available for

the media sector to the quantity of professional journalists employed by the outlet, recognised as such by the independent press council and subject to the sector's self-regulatory code. An advisory commission with members of the press and editors, the national university, and members of the Government administration analyse the criteria and oversee the 10 million annual support budget (Grand Duchy of Luxembourg, 2021[56]).

Direct funding is often limited or available for special content, such as minority language media or the promotion of specific topics. The Italian Budget Law of 2024, for example, funded a system of support for the media industry through a permanent "Single Fund for Pluralism and Digital Innovation in the Information and Media Publishing Sector." Among others, the eligibility requirements for receiving funds include minimum salary levels and staffing a minimum number of professional journalists with full-time, permanent contracts (at least four journalists for publishers of daily newspapers and at least two journalists for publishers of periodicals). Allocations will also favour publishers that recruit journalists and professionals aged 35 years or less, with professional skills in the fields of digital publishing, communication and cybersecurity, and with a focus on countering disinformation (Gazzetta Ufficiale, 2023[57]). Finland, furthermore, provides EUR 800 000 to cultural magazines and EUR 500 000 to minority language newspapers (Bleyer-Simon and Nenadić, 2021[55]). Provided the funds are allocated in a transparent, publicly accountable, and relatively predictable manner, direct subsidies can be important tools to support the media and information space (Forum on Information and Democracy, 2021[54]).

Governments may financially support private media by buying advertisements. However, such direct support must be done in a transparent and impartial way to prevent media capture by the government or elected officials. If not done transparently and impartially, state advertising can be a problematic form of support that may be used to buy or maintain political influence. Notably, within the European Union, 19 of 24 countries recently studied do not have guidelines to transparently allocate state advertising among news media (Bleyer-Simon and Nenadić, 2021[55]).

For its part, Ireland's Future of Media Commission Report recommended expanding the media sector and increasing its plurality by adapting the current Broadcasting Fund into a platform-neutral "Media Fund" to finance schemes for public service content providers, including for local news reporting and supporting the digital transformation. The report also recommends reducing tax for newspapers and digital publications and for investments in non-profit media organisations to receive tax exemptions (Government of Ireland, 2022[58]).

Support measures can also be directed at reaching vulnerable and hard to reach groups. For example, the Estonian government supports Russian language content creation, which is seen as an efficient means to provide reliable information to non-Estonian speakers in the country. This information is designed to compete with Russian state-funded propaganda aimed at the non-Estonian-speaking minority. Funding went to public broadcaster ERR as well as private media outlets. The support programme was created in co-operation with the media outlets with specific attention to freedom of expression and political neutrality (ERR, 2023[59]).

Community media is another important element in ensuring a diverse and free media environment. Community media broadly refers to broadcasting, newspapers and multimedia outlets that are independent from governments, commercial institutions and political parties and directed by and largely owned by local communities and/or communities of interest which they serve (Chapman, Bellardi and Peissl, 2020[60]). One avenue for government action is through building out the internet infrastructure to enable the growth of local and community news providers. Areas without broadband connections or with high internet connection costs have reduced economic incentives for broadcast outlets and digital start-ups to provide news and information to residents in those communities. Addressing issues around the lack of access to high-speed internet, including in places that also have lost local news sources, can (among other positive outcomes) help reduce the digital divide and strengthen the competitive field for local and community news providers (Medill Local News Initiative, 2023[40]).

The importance of community media is reiterated in the Council of Europe's Recommendation on Media Pluralism and Transparency of Media Ownership, which encourages member states to "support the establishment and functioning of minority, regional, local and not-for-profit community media, including by

providing financial mechanisms to foster their development (Council of Europe, 2018[50])." Similarly, the Organisation for Security and Co-operation in Europe (OSCE) recommends that states recognise the distinct nature of not-for-profit community media, guarantee their independence, and allow them to provide members of the communities they serve with opportunities and training that enable them to produce their own media content (OSCE, 2019[61]).

Luxembourg has put in place a financial aid mechanism of EUR 100 000 per year for community media outlets that rely on the voluntary participation of individuals in editorial activities and that support media education, integration, and social cohesion (Grand Duchy of Luxembourg, 2021[56]). For its part, as of 2020, the United Kingdom had 255 community radio stations, reaching 3.5 million local listeners and involving 20 000 volunteers (Chapman, Bellardi and Peissl, 2020[60]). In addition to adding to the diversity of a country's media ecosystem, facilitating public engagement in the production of locally relevant journalism can serve as an important venue for building media literacy.

International efforts to strengthen media and information environments

Government support for a diverse and independent media sector is also recognised as a priority for international co-operation and development. In many countries, development agencies are supporting information integrity through partnerships with local media outlets and journalists working in the field. ODA for media and information environments has increased from USD 325 million in 2002 to USD 1.2 billion in 2021. However, this represented only 0.5% of total ODA in 2021, and excluding investments in infrastructure (such as broadband and telephone connections), ODA for media and information has remained flat at around USD 500 million per year since 2008 (OECD, 2024[62]).

Development assistance to media and information generally falls within three policy areas. First is a focus on strengthening government initiatives. These projects support efforts to promote freedom of expression, media support for governance and accountability (including media sector development and the role of media in elections), access to information and government transparency, and digital democracy and internet freedoms. A second focus is on expanding access to technologies and physical infrastructure, including support for technological innovations, infrastructure (telephone and broadband), and telecommunication regulation reforms. A third category includes a focus on support to media and communication efforts to disseminate information on specific development objectives, such as around efforts to advance health, environmental or other development objectives. It also includes strategic communication programmes to disseminate information about the priorities and interests of development partners (see Box 2.5 for examples) (OECD, 2024[62]).

Box 2.5. ODA initiatives to strengthen media and information environments

In France, the Ministry of Europe and Foreign Affairs supports Canal France International (CFI), the French media co-operation agency working to encourage the development of medias in countries that receive development aid. It supports media organisations and civil society stakeholders based in these countries committed to providing free, democratic, and unbiased information, while also developing an awareness of sustainable development requirements. Since 2016, the French development agency, *l'Agence française de développement* (AFD), also has a mandate from the French Ministry of Europe and Foreign Affairs to finance projects dedicated to freedom of the press and training for journalists, strengthening of media, and efforts to counter disinformation. Among other initiatives, AFD signed a multi-year partnership agreement with Reporters Without Borders in 2022, which is being implemented in 66 countries on four continents. It includes funding for 18 local organisations in Europe, the Middle East, and North and West Africa specialising in trainings on journalist safety, fact-checking and investigative journalism.

Spain's development agency, *Agencia Española de Cooperación Internacional para el Desarrollo* (AECID), launched "*Programa Democracia*" in 2023 to support social dialogue and knowledge exchanges between Spain, other European countries, Latin America, and the Caribbean, with the objective to reinforce democratic values. One of the key pillars of this programme is the protection of human rights and fundamental freedoms via the support of journalists, activists, and academics and the defence of a diverse and pluralistic media space that favours reasoned dialogues in these regions.

The Deutsche *Gesellschaft für Internationale Zusammenarbeit* (GIZ), the German development agency, also finances projects to enhance journalistic quality and innovation of independent media organisations. Together with the European Union as co-financer and DW Akademie and Internews Europe as implementing partners, GIZ is supporting a three-year project (2022-2025) on media freedom and pluralism in the Western Balkans. The project focuses on helping independent media outlets improve their reporting and revenue-generating capacities.

In 2023, the United States Agency for International Development (USAID) launched the Pro-Info Initiative, which will provide USD 16 million to help promote digital and media literacy and support emerging technologies and "pre-bunking" efforts in countries where they operate.

Sources: (CFI, 2023[63]); (AFD, 2022[64]); (AECID, 2023[65]); (GIZ, 2022[66]); (USAID, 2023[67]).

Evaluations show that international co-operation and ODA can play a particularly important role in helping media actors survive, thus keeping citizens as well informed as possible in fragile political contexts and in conflict settings. Long-term and large investments can also have system-wide effects, such as the transformation of Ukraine's media sector. In the short- and medium-term, thematic programmes can be effective, such as shining a light on corruption and holding perpetrators to account through investigative journalism networks. Over the longer-term, supporting the capacity of journalists, strengthening media outlets, and developing the wider media enabling environment can ensure larger audiences are reached with better quality and more engaging information.

On the other hand, impact is insufficiently measured, and opportunities to develop joint donor strategies and evaluations in partner countries remain largely untapped. A 2023 study by USAID classified countries either under the so-called global north group and global south group and found a "severe imbalance" in evidence related to what works to counter misinformation in the countries classified as Global North versus those classified under Global South. The review found that 80% of the studies identified were conducted in the Global North, making it a challenge to draw conclusions about effective strategies for countering misinformation in the Global South (USAID, 2023[68]).

Evidence on how information environments benefit other development and diplomatic objectives, and how ODA programmes related to the information space can be most effective, would strengthen the political weight of international support and could lead to increases in both ODA and expert staffing. Recently, ODA supported initiatives to combat disinformation have been piloted, in particular in relation to COVID and electoral processes in partner countries, but this remains marginal as it is a new field for many donors and expertise is limited.

To support and strengthen these efforts, several normative initiatives are being developed and implemented. The OECD DAC's Network on Governance is developing updated "Principles for Relevant and Effective Support to Media and the Information Environment", and the Freedom Online Coalition adopted Donor Principles for Human Rights in the Digital Age in October 2023.[17]

Continuing to develop partnerships between development agencies, local actors, and international bodies is an important avenue to providing funding and promoting the exchange of best practices in a context where independent journalism in local languages faces eroding business models and, in some contexts, security risks and restrictions on press freedom (UNESCO, 2022[69]). For example, the U.S. Department of State Global Engagement Center (GEC) has undertaken several efforts to support independent media in those countries where it is being attacked. Separately, activities have included support for continuity of operations; trainings on journalistic skills, locally relevant studies of media capture tactics, and business sustainability planning for independent media; stakeholder mentorship; and the promotion of regional networking among entities who promote free expression. GEC also exposes disinformation narratives and tactics directly and works with foreign partners to build resiliency to foreign information manipulation and interference (FIMI).

Separately, the International Fund for Public Interest Media (IFPIM) was established in 2021 as an independent, multi-stakeholder initiative designed to address the challenges facing the media sector in low- and middle-income countries and to help identify pathways toward long-term sustainability.[18] In Europe, the Local Media for Democracy project aims to support the local media landscape with measures to build resilience, independence, and sustainability. Ultimately, via mapping news deserts in the EU and targeted media funding, the project seeks to support an enabling environment where a pluralistic and independent media landscape can exist (European Federation of Journalists, 2023[70]).

Several considerations help guide the design of government support mechanisms for media. For example, steps need to be taken to ensure the design of support models to private media, which were often created for traditional print and broadcast media, are appropriate to the new communication environment (Forum on Information and Democracy, 2021[54]). At the same time, in highly polarised societies, governmental support for public, private, or community media could be potentially used by malign actors to accuse the government of spreading false and misleading content. To mitigate such concerns, governments should ensure that there is a strong firewall between the media entity and government in terms of content and put in place clear and transparent rules for funding allocation and provide information about subsidies, project financing, and project activities. It is particularly important that procedures and control mechanisms demonstrate to the public that governmental support has no direct impact on the produced content and that political considerations do not affect distribution of financial or other support to media outlets. Similarly, when media outlets receive support from other governments or from international organisations, they run the risk of appearing to be under the control of an external actor. Any government support mechanism for media, especially support mechanisms for foreign media, must lay out clear and public rules to ensure that editorial stances are not influenced by outside assistance.

2.3.3. Strengthening economic incentives to promote better functioning online information spaces

While not directly connected to counteracting disinformation, identifying economic drivers that help provide incentives to online platforms to promote information integrity is an important approach. From a consumer perspective, while online platforms have brought substantial benefits, including lower information and communication prices, greater accessibility and convenience, and access to new content and means of engagement, several concerns

have been identified with respect to competition in digital markets. Notably, digital-intensive sectors have demonstrated a tendency toward greater market concentration and falling entry rates of new firms (OECD, 2019[71]; OECD, 2022[72]). This is partly a result of strong merger activity in these markets. For example, between 2001 and 2021, Google bought 258 companies; Facebook (now Meta) employed a similar practice, buying 90 companies in a period of 16 years (2005 to 2021), meaning they closed one deal every two months (Nadler and Cicilline, 2020[73]) (American Economic Liberties Project, 2021[74]). In addition, there are certain inherent characteristics of digital markets that make them prone to concentration, including the presence of network effects (the phenomenon through which the value of a product or service increases when more people use it), data feedback loops (which enable platforms that derive significant volumes of data from their large user bases to continually improve their products and services), and strong economies of scale.

Concentration may in turn have reduced competition for and availability of trustworthy sources of news (Nadler and Cicilline, 2020[73]). Moreover, with fewer options available to consumers, concentration may also reduce incentives for large online platforms to compete on quality aspects. These trends are a concern because evidence shows that healthy market competition helps spur innovation, as well as promote long-term growth and well-being (OECD, 2022[75]).

Several jurisdictions have implemented, or have proposed, specific policies to address competitive harms in digital markets. By encouraging new entrants and innovation, these strategies seek to spur competition between online platforms, potentially encouraging market-based incentives to healthier information spaces, though this outcome is far from certain. For example, regulations may address, as appropriate, data-related concerns, including obligations to implement data portability and interoperability measures. Enabling consumers to switch services more easily may prevent anti-competitive conduct and encourage innovation. Governments may also include issues related to the 'gatekeeper' status of online platforms, including measures to limit bundling and self-preferencing their own goods and services. Some regulators have also put in place additional merger requirements that increase scrutiny of attendant competition risks (OECD, 2022[75]).

The European Commission (EC), for example, has taken this approach through the Digital Markets Act (DMA). The EC has focused on creating and maintaining a level playing field for digital services; ensuring responsible behaviour of online platforms; fostering trust, transparency and ensuring fairness on online platforms; and keeping markets open by promoting a fairer business environment and encouraging new services to enter the market (OECD, 2022[3]).

The nature of the relationship between digital platforms and news publishers is complex. From the news publishers' perspective, this relationship is characterised by a tension between the short-term operational opportunities of using digital platforms as effective channels of distribution of news content and the long-term concern to become "too dependent" on these platforms (Nielsen and Ganter, 2018[76]). From the digital platforms' perspective, there are conflicting views as to the value of news content, particularly compared to other type of third-party content, for their businesses and revenue (OECD, 2021[77]).

In light of these dynamics, one avenue to promote competition in this space has been to put in place requirements for online platforms to remunerate news media companies for linking to content. In Australia, the news media bargaining code came into effect in March 2021. It addresses the bargaining power imbalances between specifically designated online platforms (notably, those that have a "significant bargaining power imbalance with Australian news businesses") and publishers (Australian Competition and Consumer Commission, 2020[78]). The code requires designated digital platforms to negotiate in good faith with news businesses that have registered an intention to bargain. If an agreement about remuneration cannot be reached within three months, there is a compulsory arbitration mechanism within the framework to resolve disputes over remuneration (Australian Competition and Consumer Commission, 2020[78]). A government review found that by the end of its first year of operation, more than 30 commercial agreements had been struck between digital platforms (Google and Meta) and a range of Australian news businesses outside the code. It is unlikely these agreements would have been made without the Code (Government of Australia - The Treasury, 2022[79]).

Similarly, in July 2019, France enacted a law transposing the EU directive on copyright and related rights,

including providing remuneration criteria for the use of news abstracts on online platforms (Autorité de la concurrence, 2020[80]). In April 2020, the French competition authority imposed interim measures requiring Google to negotiate in good faith with publishers and news agencies on the remuneration due to them under the law after finding that Google had likely engaged in anti-competitive conduct designed to circumvent the law (Autorité de la concurrence, 2020[80]). Furthermore, in 2023, Canada passed the Online News Act, which "aims to ensure that dominant platforms compensate news businesses when their content is made available on their services," and creates a bargaining framework to encourage platforms to reach voluntary commercial agreements with a range of news businesses, which would proceed to mandatory bargaining and arbitration process if unsuccessful (Government of Canada, 2023[81]).

The potential downsides to this approach can be seen, however, in the restrictions to free and open linking across the internet imposed by the regulations, and the risk that online platforms remove access to professional and traditional news sources in particular jurisdictions entirely. Indeed, Meta announced that "people in Canada will no longer be able to view or share news content on Facebook and Instagram," as the value Meta receives from allowing users to post links to news articles is less than the cost for paying the outlets for links that were previously made voluntarily (Meta, 2023[82]). Moving forward, the aim will be to continue to identify approaches that support an independent and diverse media sector, while upholding a free and open information space.

2.4. COUNTERING SPECIFIC RISKS IN THE INFORMATION SPACE

Given the dynamic global information space, the fast-paced technological innovation shaping it, and increasing geopolitical tensions, risks to the information spaces are rapidly evolving, with new risks emerging or new opportunities for those aiming to perpetrate disinformation campaigns. In this context, reinforcing information integrity demands that policymakers pay close attention to political, economic, technological or societal trends that can affect the risk landscape in this area.

While not new, the threat of foreign information manipulation and interference (FIMI) has continued to grow as malign actors use new technologies in novel ways. Off-the-shelf generative AI tools will enable more tailored FIMI operations by a broader range of actors, enabling the creation of higher quality content, at greater speed and scale, and at lower cost. The 2nd EEAS Report on Foreign Information Manipulation and Interference Threats found that FIMI threat actors strategically and opportunistically make use of the attention created by certain events, such as elections, emergencies, and political summits to pursue their interests (EEAS, 2024[83]). 2024, the so-called super election year – with more than 4 billion people likely to vote – will offer increased opportunities for malevolent actors to interfere in elections and try to shape political outcomes.

These examples showcase the importance of designing specific policy responses for these novel or emerging threats. Together, foreign interference fuelled by geopolitical tensions, the largest election year in history, and the power of generative AI becoming easily accessible elevate the level of information integrity risks. In this context, building understanding of the scope of the challenges and identifying policy responses could focus on:

- Responding to the threats posed by the spread of foreign information manipulation and interference (FIMI)
- Strengthening the information space in the context of elections by providing timely and reliable information to the public on how to exercise their rights, and
- Responding to the changes introduced by generative AI to the information space.

2.4.1. Risks posed by foreign information manipulation and interference

An important avenue for strengthening the information space is to recognise and respond to threats of foreign malign interference. If done transparently through official channels, foreign influence is legal and can contribute to democratic debates. Risks to democratic processes arise, however, from efforts by foreign agents to interfere in democratic processes and information spaces in ways that undermine decision-making, reduce

trust in democratic systems, increase polarisation, and that hide the actors' activities and intent.

While a single, universally accepted definition of foreign interference does not yet exist, the concept broadly refers to efforts by foreign actors to interfere illegitimately in decision-making processes of a target country. It encompasses actions both by state and non-state actors, as well as their proxies. Foreign interference is also marked by the co-ordination of activities and the malign nature of actions that seek to negatively impact values, procedures, and political processes. While all governments seek to influence deliberations on issues of importance to them as part of their foreign policy toolbox, globalisation and digitalisation have amplified the challenge of foreign interference and made it much more of a civilian concern, with open democracies being more fragile to foreign interference than more closed systems. Several governance loopholes can be addressed in this regard to make democracies more resilient to foreign interference.

In the information space, foreign information manipulation and interference (FIMI) seeks to shape public opinion and discourse, often with the aim of strengthening parallel interference efforts (see Box 2.6 for definitions). Foreign malign actors often seek to exploit global information flows to gain influence, affecting countries globally, contributing to democratic backsliding, and threating political instability and violent conflict through disinformation campaigns (Office of the Director of National Intelligence, 2023[84]).

Domestic or foreign actors may spread disinformation as part of a foreign malign influence operation. Domestic actors can act as the witting or unwitting proxies of foreign malign actors, motivated by political, economic, social, or monetary gains. A key objective of FIMI actors is to destabilise society and government within the target state and confuse public debate around key issues, with disinformation often to be designed to be spread through domestic discussion and online. One tactic used to achieve this is exacerbating existing political and social fissures. This approach allows foreign actors to achieve more effective and seemingly authentic outreach, to save resources, and to hide the origins of the interference activities.

Box 2.6. Defining foreign interference and Foreign Information Manipulation and Interference (FIMI)

Toward a definition of foreign interference

The concept of "foreign interference" is broad. For example, the European Parliament's definition notes that "foreign interference is illegitimate interference in the politics and democracy of the European Union and its Member States by foreign powers" (European Parliament, 2023[85]).

For its part, the United States Department of Homeland Security (DHS) defines foreign interference as "malign actions taken by foreign governments or foreign actors designed to sow discord, manipulate public discourse, discredit the electoral system, bias the development of policy, or disrupt markets for the purpose of undermining the interests of the United States and its allies" (United States Department of Homeland Security, 2018[86]), while the United States Code uses the term "foreign malign influence", defined in 50 USC § 3059(e)(2), as "any hostile effort undertaken by, at the direction of, or on behalf of or with the substantial support of, the government of a covered foreign country with the objective of influencing, through overt or covert means, (A) the political, military, economic, or other policies or activities of the United States Government or State or local governments, including any election within the United States; or (B) the public opinion within the United States."

The Australian Attorney General's Department understands the concept of foreign interference as "covert, deceptive and coercive activities intended to affect an Australian political or governmental process that are directed, subsidised or undertaken by (or on behalf of) foreign actors to advance their interests or objectives" (Australian Government Attorney-General's Department, 2019[87]).

A common understanding and definition of foreign interference could be useful to distinguish it from legitimate foreign influence and reduce the risk of foreign interference through international co-operation. Based on existing national definitions in OECD countries, common elements of foreign interference activities generally include the lack of transparency of the activities conducted; that the activities are conditioned, tasked or instructed, directly or indirectly, by a foreign state; and that they are intended to be harmful to the target country.

Foreign Information Manipulation and Interference (FIMI)

The European Union uses the term "foreign information manipulation and interference" (FIMI), which mainly focuses on disinformation threats, but is also related to the broader foreign interference picture: "Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and co-ordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory" (European External Action Service, 2023[88]).

Source: European Parliament (2023[85]), Legal loopholes and the risk of foreign interference. In depth-analysis requested by the ING2 special committee, https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702575/EXPO_IDA(2023)702575_EN.pdf; United States Department of Homeland Security (2018[86]), *Foreign Interference Taxonomy*, https://www.cisa.gov/sites/default/files/publications/foreign_interference_taxonomy_october_15.pdf; Australian Government Attorney-General's Department (2019[87]), *Foreign Influence Transparency Scheme. Factsheet 2 "What is the difference between 'foreign influence' and 'foreign interference'?"*, https://www.ag.gov.au/sites/default/files/2020-03/influence-versus-interference.pdf; European External Action Service (2023[88]), *1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a framework for networked defence*, https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en.

FIMI operations often seek to influence specific domestic and foreign policy decisions of target states, sow divisions in societies, denigrate democratic values, processes and institutions, and rally support for the policies of the perpetrating state (EEAS, 2023[89]). Foreign and malign information initiatives also seek to weaken target states by targeting foreign policy interests, as well as reducing the population's trust in government institutions, widening political cleavages and societal polarisation, and undermining democratic resilience (U.S. Department of State, 2020[90]) (OECD, 2022[91]).

Foreign state actors have also used a wide range of channels, tools, and practices to create and spread disinformation through potentially vast networks consisting of official, proxy, and unattributed communication channels, including state-backed media, global television networks, fake social media accounts and fake news websites. One avenue is via state-owned and controlled media of authoritarian states, such as Sputnik, RT, and TASS in Russia, and Xinhua and CCTV in China. The importance of these channels can be seen in Russia, for example, where government spending on "mass media" for the first quarter of 2022 was 322% higher than for the same period in 2021, reaching 17.4 billion roubles (roughly EUR 215 million). Almost 70% of Russia's spending on mass media in Q1 2022 was spent in March, immediately after Russia's invasion of Ukraine (The Moscow Times, 2022[92]). The outlets that receive these funds, including RT and Rossiya Segodnya, which owns and operates Sputnik and RIA Novosti, are state-linked and state-owned outlets that "serve primarily as conduits for the Kremlin's talking points and can be more accurately thought of as tools of state propaganda (United States Department of State, 2022[93]) (Cadier et al., 2022[94]).

The Chinese government has expanded the distribution of content favourable to its positions through the reach of its state-owned media, purchasing foreign media outlets, and by publishing favourable content in foreign media outlets. For example, as noted in the U.S. Department of State GEC report "How the People's Republic of China Seeks to Reshape the Global Information Environment," Xinhua, the Chinese government's official state news agency, maintained 181 bureaus in 142 countries and regions as of August 2021. The Chinese government has also purchased controlling stakes in media outlets in Europe, Asia, and Africa, in many cases evading media transparency rules and often shifting news and editorial coverage to more pro-Chinese positions (U.S. Department of State, 2023[95]). In addition, government-controlled media has used content-sharing agreements with foreign local media outlets to supply information products for free or at heavily subsidised prices to local media outlets, and in some cases prohibiting recipients from entering into content-sharing agreements with Western-sourced wire services. Such an approach can discretely promote pro-Chinese positions while limiting the reach of other outlets. These types of agreements – in which information provided by Chinese outlets appears in local media without attribution – risks distorting information environments and reduces the ability of citizens to make transparently informed decisions (U.S. Department of State, 2023[95]).

In response, for example, the Baltic states were the first EU countries to impose temporary bans on the broadcasting of some Russian TV channels, directly or indirectly run by the Russian state, which actively spread disinformation, propaganda and incitement to hatred. Following Russia's war of aggression against Ukraine in 2022, the European Union introduced a Union-wide ban on broadcasting of the two Russian state-run channels, RT (Russia Today) and Sputnik. In December 2022, the European Union expanded the list of banned Russian TV channels to address the "systematic, international campaign of media manipulation and distortion of facts in order to enhance its strategy of destabilisation of its neighbouring countries, and of the Union and its Member States (Official Journal of the European Union, 2022[96])."

Malign actors also use cyber-attacks to steal and distribute sensitive information as a more active effort to support wider disinformation campaigns. For example, prior to the 2017 French presidential election, a co-ordinated attempt to undermine Emmanuel Macron's candidacy included the hacking and leaking two days before the second and final round of the presidential election of more than 20 000 emails stolen from the computers of campaign staff. This cyber-attack was timed to coincide with the campaign blackout period which prevents campaigning mandated by law and was co-ordinated with a disinformation campaign that in parallel spread rumours and forged documents. On X alone, a co-ordinated effort to spread related content by promoting the hashtag #MacronLeaks

appeared in almost half a million tweets in twenty-four hours (Vilmer, 2019[97]). In addition to the harms caused by illegally accessing private information and the risks posed by cyber-attacks to democratic processes more widely, this campaign highlights how malign actors can use hacked governmental data, commercial secrets, and personal information to obscure and undermine public debate.

Actors can use opportunities provided by online platforms to amplify the reach of content to spread foreign information manipulation and interference campaigns. Beyond hijacking social platform accounts of elected or other public officials, malign actors pursue less overt means of artificial amplification, including by stealing accounts and creating "bot farms" to spread content. This co-ordinated exploitation of accounts post, share, and like target materials in ways that mimic – and may then develop into – actual engagement on platforms and even spread to off-line news sources.

Moving forward, generative AI technologies will provide greater opportunities for the creation and distribution of false and misleading content. Malign actors may use these rapidly evolving technologies to generate realistic looking and difficult to detect automatically fake user profiles, text, audio, and video materials, as well as to manage bot networks. To this end, foreign information manipulation and interference should be seen as part of larger efforts to undermine democratic processes. Disinformation efforts are an important national security tool for nations and nonstate actors whose goal it is to undermine democracy (Danvers, 2023[98]). Attacks against elected and public officials and candidates can directly distort the political process. Undermining citizens' perception of the fairness, transparency, and security of the electoral process erodes trust in democratic system more widely. Maintaining information integrity is therefore a key measure to upholding the integrity of democracies.

Existing policies to counter foreign interference can be applied to new communication technologies and challenges

Disinformation activities benefit from ambiguity and obscurity; using transparency enforcement mechanisms can facilitate disclosures and provide an avenue to punish covert and malign foreign interference by government actors. To that end, applying existing regulation to counter foreign interference to new communication technologies and challenges is a promising policy response. For example, in the United States, the application of the Foreign Agents Registration Act (FARA), which originally passed in 1938, shows how existing legislation to increase transparency of foreign governments' influence activities can be adapted for use in combatting the spread of disinformation online. In 2018, the United States indicted 13 Russian nationals and three Russian companies (the Internet Research Agency LLC, Concord Management and Consulting LLC, and Concord Catering) under FARA for creating false accounts, concealing advertising, and organising and co-ordinating political rallies in an effort to interfere in the U.S. elections (United States Department of Justice, 2022[38]) (Box 2.7).

Box 2.7. The application of the Foreign Agents Registration Act (FARA) to the fight against disinformation

U.S. Congress passed the Foreign Agents Registration Act (FARA) in 1938 to increase transparency of foreign governments' influence activities. The Foreign Agents Registration Act Unit, which is part of the U.S. Department of Justice's National Security Division, administers and enforces FARA.

The Act requires any actors (political agents, lobbyists, public relations counsel, fundraisers, corporations, organisations, among others) working on behalf of or in the interest of a foreign government or foreign principal outside of the United States, including Americans, to disclose their affiliations and activities as well as receipts and disbursements in support of those activities. One of the main goals of the Act is to fight against the use of propaganda activities by making efforts of foreign actors easier to identify by the U.S. Government and public. "Political activities" covered by FARA include any activity that the actor believes will or intend to influence the government regarding its domestic and foreign policies.

While FARA has been a tool to combat foreign propaganda and influence campaigns for several decades, the government has more recently used it to prevent covert foreign disinformation activities. For example, in 2017, the Florida-based company RM Broadcasting was providing a platform for the broadcast of radio programmes from a Russian state-owned news agency, thus acting as an agent of a foreign principal, even though it was not registered as such. RM Broadcasting was ordered to register under FARA to make it easier for radio listeners to understand the source of their news. In 2018, furthermore, several Russian nationals and Russian companies were charged with attempted interference of the 2016 U.S. Presidential election; a basis of the indictments was the agents' failure to comply with FARA.

While the scope of FARA is broad, there are several exceptions for accredited diplomatic or consular officers, actors engaging in bona fide trade or commerce activities, religious, scholastic, academic, or scientific pursuits or fine arts. As the risk posed by the spread of disinformation, particularly by foreign actors, has been further recognised in the United States as a priority in recent years, criminal proceedings against actors who failed to register under FARA have also increased.

Source: The United States Department of Justice (2023[99]), Foreign Agents Registration Act, https://www.justice.gov/nsd-fara; The United States Department of Justice (2022[100]), Court finds RM broadcasting must register as a foreign agent, https://www.justice.gov/opa/pr/court-finds-rm-broadcasting-must-register-foreign-agent; The United States Department of Justice (2021[101]), Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere

Similarly, in Australia, the Foreign Influence Transparency Scheme seeks to provide the public with visibility of the nature, level and extent of foreign influence on Australia's government and politics (Government of Australia, 2023[102]). It does this by requiring individuals and entities who undertake registrable activities on behalf of a foreign government for the purpose of influencing Australian political or governmental processes to disclose these details on a public register. Specifically, the scheme includes communications activities as a registrable activity to ensure people consuming information are aware of its source.[19] The scheme is not designed specifically to combat mis- and disinformation; however by making the source behind the communication activities transparent, such schemes can provide useful options to illuminate covert and potentially malign communication activities, ultimately building trust in the information space more broadly.

2.4.2. Disinformation in the context of elections

When disinformation operations are strategically conducted during electoral cycles, they directly interfere with the essential core of democracy, can undermine the trust placed in the electoral process and the bodies in charge of it, discredit political opponents, increase the risk of disputed election results and sow social unrest (UNDP, 2023[103]); (International IDEA, 2024[104]).

According to an IPSOS and UNESCO survey conducted in 16 countries where general elections will be held in 2024, 87% of respondents expressed concern about the impact of disinformation on upcoming elections in their country, with 47% being "very concerned" (IPSOS, UNESCO, 2023[105]). In addition, an increasingly digital environment brings new benefits and dangers in the context of elections. Technology can increase citizens' opportunities to find useful information for their voting decisions and foster voter mobilisation. At the same time, technology-enabled solutions can also be used to influence the electorate by spreading disinformation, for instance through artificial amplification or AI-generated deepfakes and political micro-targeting.

As elections are usually planned and their dates well-known in advance, disinformation propagators can have time to organise sophisticated operations. In addition, elections can indeed be seen as an "ideal high-impact opportunity" to conduct their information influence operations (Polyakova and Fried, 2019[106]). It is important also to note that engaging in electoral interference strategies and activities do not necessarily necessitate tangible impacts on the results of the elections to have a negative impact: sometimes casting doubts on the legitimacy of the elected candidate can achieve the expected results by those interfering. In this context, it is also important to prepare a policy response, so that detection capacities can be deployed as early as possible to reduce the risk of interference. This said, it is important to highlight that no measure to tackle disinformation during elections should interfere with legitimate political debates or justify disproportionate measures restricting the free flow of information, including the blocking of content or Internet access (UNESCO, 2022[107]).

Given the role that elected officials, candidates, and political parties play in the information ecosystem, including in generating and amplifying content, and in some cases amplifying disinformation, reiterating the importance of information integrity in elections can play a key role. The Code of Conduct Transparency Online Political Advertisements developed by the Netherlands in 2021, for example, sought to prevent the spread of misleading information during elections by receiving commitments from platforms and political parties to acknowledge a responsibility in maintaining the integrity of elections and to avoid disseminating misleading content (Government of the Netherlands, 2021[7]).

A response to the threat of information manipulation in the context of elections includes the development of a wide range of government competences, often through the creation of specialised task forces, focused on justice, national security and defence, public communication, and election management which would ideally be established well ahead of the planned elections (see Box 2.8). Stakeholders on election frontlines, including independent electoral management bodies (EMB), political parties and candidates, journalists, and civil society organisations, need to be aware of the risks that disinformation poses to free and fair elections.

A key focus of efforts focused on countering electoral disinformation is around facilitating co-operation and co-ordination across governments to share information about relevant threats and deploy appropriate response strategies. Co-ordination enables relevant offices to work together to take appropriate action while respecting political neutrality. Governments can also focus on building the public's long-term understanding of disinformation flows and risks and enhance preparedness ahead of elections. Civic education on a country's electoral legal framework prevents information gaps that can be exploited by disinformation propagators. More broadly, voter education can help safeguard electoral integrity on issues such as campaign finance and advertising rules.

Government efforts in this space also enable short-term reactions to immediate information threats in the context of electoral disinformation. In recent Brazilian elections, the judiciary co-ordinated with digital platforms to facilitate engagement and compliance of court decisions around illegal content. In this way, the Brazilian government sought to establish open and agile dialogue channels during electoral periods between digital platforms and public authorities, while ensuring that any decisions taken with regards to content moderation were made in a transparent, public manner and in accordance with the country's laws.

In addition, government offices and task forces may provide timely and reliable information to citizens on how to exercise their rights, including voter registration and election day voting procedures, particularly in response to specific disinformation campaigns (International IDEA, 2023[108]).

Box 2.8. Ensuring information integrity during elections via special taskforces

Electoral Integrity Assurance Taskforce – Australia

In Australia, the Electoral Integrity Assurance Taskforce (EIAT), made up of agencies across federal government, was established in 2018 to provide information and advice to the Australian Electoral Commissioner on matters that may compromise the real or perceived integrity of an Australian federal election or referendum. Potential threats to electoral integrity can come in the form of cyber or physical security incidents, disinformation campaigns, and through perceived or actual interference in electoral processes. Notably, this taskforce focuses on referring information about relevant threats to the appropriate agencies in Australia and facilitates co-operation and co-ordination, enabling them to work together to take appropriate action while respecting strict political neutrality.

The Taskforce and its Board are comprised of the following agencies: Australian Electoral Commission, Department of Finance, Department of Prime Minister and Cabinet, Department of Infrastructure, Transport, Regional Development, Communications, and the Arts, Attorney-General's Department, Department of Home Affairs, the Australian Federal Police, the Australian Signals Directorate, the Australian Transaction Reports and Analysis Centre, Department of Foreign Affairs and Trade, the Australian Security Intelligence Organisation, and the Office of National Intelligence.

The work of this task force is also complemented by AEC-led campaigns such as "Stop and Consider", encouraging voters to think critically about the sources of electoral information they see or hear, and the AEC Disinformation Register, focusing on harmful disinformation related exclusively to the procedural aspects of conducting elections and referendums.

Electoral Justice Permanent Programme on Countering Disinformation – Brazil

Brazil's Electoral Justice Permanent Programme on Countering Disinformation was established by the Superior Electoral Court (TSE) in August 2021, building on a similar programme established in 2019 that sought to prevent and combat the spread of mis- and disinformation about the 2020 elections.

To respond to the challenges that disinformation imposes on the integrity of elections and on democracy more widely, the Programme has adopted a "network" model, bringing together representatives from government agencies, press and fact-checking organisations, Internet providers, civil society organisations, academia, and political parties. 154 partners take part currently.

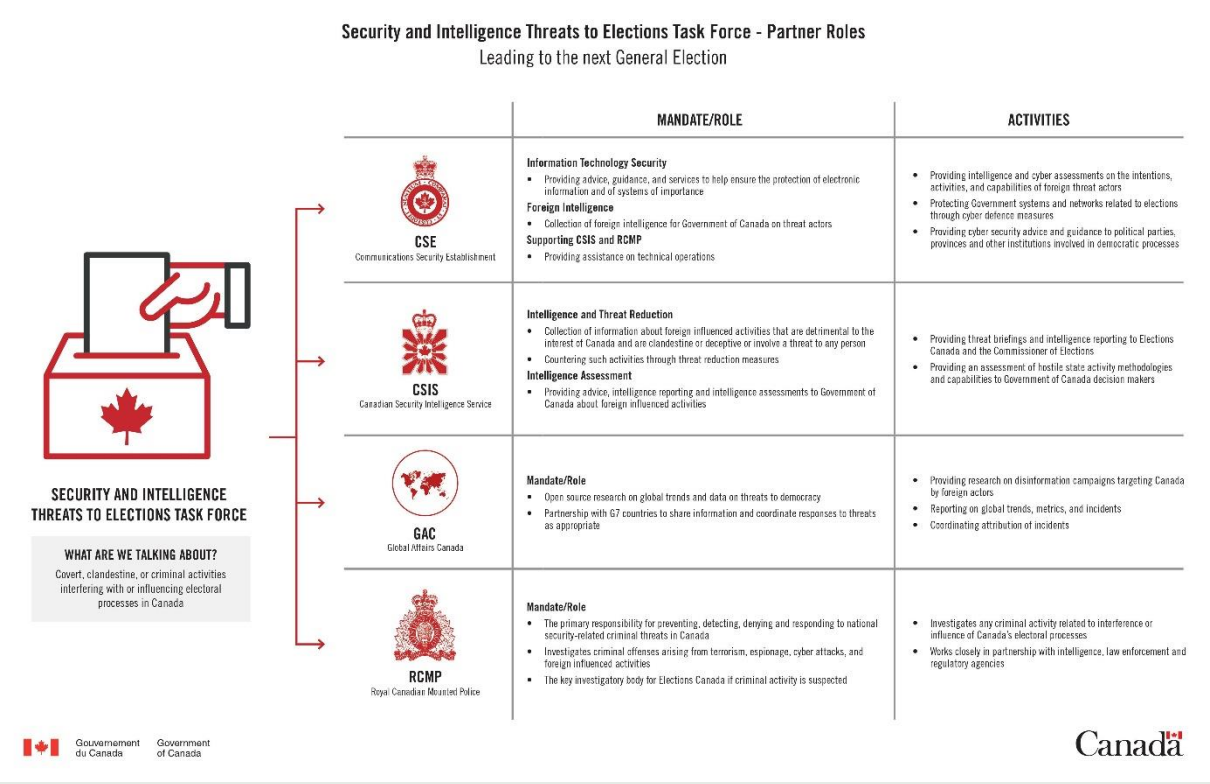
The Programme focuses on three actions: (i) Informing, which seeks to disseminate official, reliable, and quality information related to the electoral process; (ii) Empowering, which is aimed at media literacy and building societal understanding of both the threats posed by the spread of disinformation as well as civic education around the functioning of the electoral process in Brazil; and (iii) Responding, which is focused on identifying disinformation campaigns and countering its negative effects.

Critical Election Incident Public Protocol & Security and Intelligence Threats to Elections (SITE) Task Force – Canada

In anticipation of the 2019 election, Canada put in place the Plan to Protect Canada's Democracy presenting concrete actions to safeguarding democratic institutions and processes. The Plan includes four pillars of action: enhancing citizens' preparedness, enhancing organisational readiness, combating foreign interference, and building a healthy information ecosystem.

As a result of this Plan, Canada established a Critical Election Incident Public Protocol, which lays out a simple, clear, and impartial process by which Canadians would be notified of a threat to the integrity of a General Election.

Canada also established a Security and Intelligence Threats to Election (SITE) Task Force to identify and prevent covert, clandestine, or criminal activities from influencing or interfering with Canada's electoral process. The primary responsibilities of the Task Force are to raise awareness of foreign threats to Canada's electoral process and to prepare the government to assess and respond to those threats, including disinformation campaigns. The Task Force comprises representatives from the Communications Security Establishment, the Royal Canadian Mounted Police, Global Affairs Canada, and the Canadian Security Intelligence Service.



Source: Australian Electoral Commission (2023[109]), "Electoral Integrity Assurance Taskforce", https://www.aec.gov.au/about_aec/electoral-integrity.htm; Government of Brazil Electoral Justice Permanent Programme on Countering Disinformation Strategic Plan 2022, https://international.tse.jus.br/en/misinformation-and-fake-news/tse-brazil-counter-disinformation-program-2022-f.pdf; Government of Canada (2021[110]), "Security and Intelligence Threats to Elections (SITE) Task Force", https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html; Government of Canada (2023[111]), "Rapid Response Mechanism Canada: Global Affairs Canada", https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/index.aspx?lang=eng.

2.4.3. Governments will need to respond to the changes introduced by generative AI to the information space

While risk-based regulation is increasingly used to mitigate the risks in the role that online platforms play in spreading information (including mis- and disinformation), such an approach should also respond to the role of Artificial Intelligence (AI) tools and systems, how those affect the information space, and how they are used as a disinformation tool that undermines human rights, for example by being used to silence women and members of marginalised communities participating in public life. The rapid development of advanced AI systems has indeed the potential to lead to innovations that can both benefit societies, while also posing new risks (GPAI, 2023[112]).

In the information space, generative AI[20] tools may help identify inauthentic accounts or patterns, thereby helping governments improve their situational awareness around disinformation campaigns and complementing the moderation work by digital platforms. The tools may also be used to support the

development of educational materials and activities, as well as to facilitate translation, summaries, and analysis, greatly facilitating and reducing the cost of these activities for public officials, journalists, and CSO actors alike (Landemore, 2023[113]).

The ability for generative AI to create and disseminate highly convincing content also raises the risk posed by rapid growth of realistic false or misleading news, articles, and visual media, posing an additional risk to people's trust in the information space, particularly online. In addition to content generation, generative AI could also help create a large amount of realistic fake profiles on online platforms, help animate networks of fake accounts, and overcome the detection capabilities recently created by governments, platforms or other stakeholders to identify co-ordinated inauthentic behaviour on platforms. By vastly reducing the cost of and language barriers to creating convincing text or visuals, and by making it increasingly difficult to distinguish between genuine and manipulated content, generative AI tools have the potential to magnify the challenges already introduced by online platforms. This situation may further erode the foundation of trust that individuals place in the information they consume, leading to heightened scepticism and uncertainty.

To that end, the OECD Recommendation on Artificial Intelligence calls for AI actors to commit to transparency and responsible disclosure regarding AI systems in order to: 1) foster a general understanding of AI systems; 2) ensure stakeholders are aware of their interactions with AI systems, including in the workplace; 3) enable those affected by an AI system to understand the outcome; and 4) enable those adversely affected by an AI system to challenge its outcome and understand the logic that served as the basis for the prediction, recommendation, or decision (OECD, 2019[114]).

Regarding the potential impact on the information space more specifically, focusing on generative AI tools (as opposed to the wider universe of AI applications and effects related to autonomous weapons, facial recognition technology, self-driving cars, and economic impacts), is a helpful framework for analysis. Policies could consider requiring that consumer-facing generative AI systems make public the training data used to build the systems, ensuring that the principles used to guide the tools are available to allow for comparison between tools and public oversight of what guardrails systems have put in place (or not, as the case may be), and watermarking of content produced (Giansiracusa, 2023[115]).

Along these lines, the proposed EU AI Act, presently under discussion, follows a risk-based approach and establishes obligations for providers and users depending on the level of risk the AI can generate. On the one hand, the EU AI Act will seek to prohibit AI systems with an "unacceptable level of risk to people's safety", including systems that "deploy subliminal or purposefully manipulative techniques, exploit people's vulnerabilities or are used for social scoring (classifying people based on their social behaviour, socio-economic status, personal characteristics)" (European Parliament, 2023[116]). The act would also require the creation of risk assessment and mitigation plans and require that generative AI tools follow transparency requirements, such as disclosing what content was generated by AI. The EU AI Act would also require tools to be designed to prevent the generation of illegal content and to publish summaries of copyrighted data used for training (European Parliament, 2023[116]). The EU's approach in this space illustrates how the application of a risk-based approach can inform other regulatory responses to technologies that play an important role in the information space beyond online and social media platforms. Similarly, governments have sought to counter the risks posed by deepfakes, audio or visual media content that seem authentic but are in fact synthetic or manipulated.

Deepfakes present a disinformation risk by presenting believable, though fake, images and audio. While synthetic media is not new, the access to technology, scale, speed, and quality of deepfakes has increased a focus on the role of policy responses. Many of the efforts to prevent risks posed by deepfakes seek to enhance transparency around the content itself and the processes followed by the systems to help validate provenance and accuracy, as well as to build on existing legal restrictions on content use. An approach focused on transparency can avoid regulatory overreach that may limit the technology's use for protected speech, such as satire. Along those lines, the EU 2022 Strengthened Code of Practice on Disinformation commits signatories that develop or operate AI systems to report on their policies for countering prohibited manipulative practices that generate or manipulate content (such as deepfakes). In addition, many of the laws passed in US states have focused on non-

consensual deepfake pornography given the clear harms caused and limited speech benefits. In this regard, nine states have enacted laws that regulate deepfakes, mostly in the context of pornography and elections influence (Poritz, 2023[117]). In 2023, furthermore, the Office of the President of the United States issued an *Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*, which specifically seeks in part to protect individuals from "AI-enabled fraud and deception by establishing standards and best practices for detecting AI-generated content and authenticating official content (U.S. White House, 2023[118])."

Ultimately, by identifying, analysing, and prioritising relevant risks, taking a risk-based approach can help ensure regulation is targeted and proportional, and that it does not introduce burdensome rules with little positive impact (OECD, 2021[14]). In the information space, such an approach aims to better understand, flag, and mitigate proactively the risks posed by relevant actors and to encourage or require actors to put in place mechanisms and processes that limit the risks posed by disinformation and build trust in the information space.

2.5. CONSIDERATIONS AND PATH FORWARD

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, journalists 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.

REFERENCES

AECID (2023), "Democracy Programme", Spanish Agency for Development Cooperation, https://www.aecid.es/programa-democracia. [65]

AFD (2022), "Comment le groupe AFD contribue à la liberté d'information dans le monde", Agence française de développement, https://www.afd.fr/fr/actualites/comment-le-groupe-afd-contribue-la-liberte-dinformation-dans-le-monde. [64]

American Economic Liberties Project (2021), *Big Tech Merger Tracker*, https://www.economicliberties.us/big-tech-merger-tracker/. [74]

Australian Competition and Consumer Commission (2020), *Draft news media bargaining code*, https://www.accc.gov.au/by-industry/digital-platforms-and-services/news-media-bargaining-code/news-media-bargaining-code. [78]

Australian Competition and Consumer Commission (2019), *Digital Platforms Inquiry Final Report*, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf. [24]

Australian Electoral Commission (2023), *Electoral Integrity Assurance Taskforce*, https://www.aec.gov.au/about_aec/electoral-integrity.htm (accessed on 31 August 2023). [109]

Australian Government (2023), *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023—guidance note*, Australian Government - Department of Infrastructure, Transport, Regional Development, Communications and the Arts, https://www.infrastructure.gov.au/department/media/publications/communications-legislation-amendment-combatting-misinformation-and-disinformation-bill-2023-guidance. [25]

Australian Government Attorney-General's Department (2019), *Foreign Influence Transparency Scheme. Factsheet 2 "What is the difference between 'foreign influence' and 'foreign interference'?"*, https://www.ag.gov.au/sites/default/files/2020-03/influence-ve. [87]

Autorité de la concurrence (2020), *Related rights: the Autorité has granted requests for urgent interim measures presented by press publishers and the news agency AFP (Agence France Presse)*. [80]

Baldwin, R., M. Cave and M. Lodge (2011), *Understanding Regulation*, Oxford University Press, https://doi.org/10.1093/acprof:osobl/9780199576081.001.0001. [5]

Bleyer-Simon, K. and I. Nenadić (2021), *News Media Subsidies in the First Wave of the COVID-19 Pandemic – A European Perspective*. [55]

Brennen, J. and M. Perault (2021), *How to increase transparency for political ads on social media*, Brookings, https://www.brookings.edu/articles/how-to-increase-transparency-for-political-ads-on-social-media/. [30]

Cadier et al. (2022), *Russia-Ukraine Disinformation Tracking Center*, https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/. [94]

Campbell, A. (2019), *How data privacy laws can fight fake news*, https://www.justsecurity.org/65795/how-data-privacy-laws-can-fight-fake-news/. [21]

CFI (2023), "Our mission", Canal France International, https://cfi.fr/en/content/our-mission. [63]

Chapman, M., N. Bellardi and H. Peissl (2020), *Media literacy for all: Supporting marginalised groups through community media*. [60]

Council of Europe (2023), *Good practices for sustainable news media financing*, https://rm.coe.int/msi-res-2022-08-good-practices-for-sustainable-media-financing-for-sub/1680adf466. [53]

Council of Europe (2021), *Content Moderation: Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation*, https://rm.coe.int/content-moderation-en/1680a2cc18. [11]

Council of Europe (2018), *Recommendation CM/Rec(2018)1 of the Committee of Ministers to member States on media pluralism and transparency of media ownership*, https://www.coe.int/en/web/freedom-expression/adopted-texts/-/asset_publisher/m4TQxjmx4mYl/content/recommendation-cm-rec-2018-1-1-of-the-committee-of-ministers-to-member-states-on-media-pluralism-and-transparency-of-media-ownership. [50]

Council of Europe (2016), *Recommendation CM/Rec(2016)4 of the Committee of Ministers to member States on the protection and journalism and safety of journalists and other media actors*, https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2016-4-of-the-committee-of-ministers-to-member-states-on-the-protection-of-journalism-and-safety-of-journalists. [37]

Craufurd Smith, R., B. Klimkiewicz and A. Ostling (2021), "Media ownership transparency in Europe: Closing the gap between European aspiration and domestic reality", *European Journal of Communication*, Vol. 36(6), pp. 547–562, https://doi.org/10.1177/0267323121999523. [48]

Danvers, W. (2023), *Disinformation may be one of Russia and China's greatest weapons*, https://thehill.com/opinion/national-security/3932031-disinformation-may-be-one-of-russia-and-chinas-greatest-weapons/. [98]

Douek, E. (2021), "Governing Online Speech: From "Posts-as-Trumps" to Proportionality and Probability", *Columbia Law Review*, Vol. 121/No. 3, https://columbialawreview.org/content/governing-online-speech-from-posts-as-trumps-to-proportionality-and-probability/. [19]

EEAS (2024), *2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence*, https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en. [83]

EEAS (2023), *1 st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a framework for networked defence*, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf. [89]

Ellger, F. et al. (2021), *Local Newspaper Decline and Political Polarization - Evidence from a Multi-Party Setting*, Center for Open Science, https://doi.org/10.31219/osf.io/nhwxs. [41]

ERR (2023), *Estonian Russian-language private media receive €1 million from state*, https://news.err.ee/1608898790/estonian-russian-language-private-media-receive-1-million-from-state. [59]

European Audiovisual Observatory (2016), *Media ownership - Market realities and regulatory responses*, https://rm.coe.int/media-ownership-market-realities-and-regulatory-responses/168078996c. [45]

European Commission (2023), *Code of Practice on Disinformation: New Transparency Centre provides insights and data on online disinformation for the first time*, https://ec.europa.eu/commission/presscorner/detail/en/mex_23_723. [9]

European Commission (2022), *European Media Freedom Act: Commission proposes rules to protect media pluralism and independence in the EU*, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5504. [52]

European Council (2022), *The General Data Protection Regulation*, https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/. [22]

European Court of Human Rights (2001), *Thoma v. Luxembourg*. [49]

European External Action Service (2023), *1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a framework for networked defence*, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023.pdf. [88]

European Federation of Journalists (2023), *Local Media for Democracy*, https://europeanjournalists.org/local-media-for-democracy/. [70]

European Parliament (2023), *AI Act: a step closer to the first rules on Artificial Intelligence*, https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence. [116]

European Parliament (2023), *Legal loopholes and the risk of foreign interference. In depth-analysis requested by the ING2 special committee*, https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702575/EXPO_IDA(2023)702575_EN.pdf. [85]

European Union (2022), *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*, Publications Office of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?ur. [13]

FATF (2023), *Guidance on Beneficial Ownership for Legal Persons*, Financial Action Task Force, Paris, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-Beneficial-Ownership-Legal-Persons.html. [51]

Forum on Information and Democracy (2021), *A New Deal for Journalism*, https://informationdemocracy.org/wp-content/uploads/2021/06/ForumID_New-Deal-for-Journalism_16Jun21.pdf. [54]

Forum on Information and Democracy (2020), *Working Group on Infodemics: Policy Framework*, https://informationdemocracy.org/wp-content/uploads/2020/11/ForumID_Report-on-infodemics_101120.pdf. [27]

Gazzetta Ufficiale (2023), *LEGGE 30 dicembre 2023, n. 213.*, https://www.gazzettaufficiale.it/eli/gu/2023/12/30/303/so/40/sg/pdf. [57]

Giansiracusa, N. (2023), *Three Easy Ways to Make Chatbots Safer*, https://www.scientificamerican.com/article/three-easy-ways-to-make-ai-chatbots-safer/. [115]

GIZ (2022), *Support to Media Freedom and Pluralism in the Western Balkans*, https://www.giz.de/en/worldwide/114194.html. [66]

Goldman, E. (2022), "The Constitutionality of Mandating Editorial Transparency", *Hastings Law JournalHa*, Vol. 75/5, https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=3985&context=hastings_law_journal. [26]

Government of Australia (2024), "Online misinformation", Australian Communications and Media Authority, https://www.acma.gov.au/online-misinformation. [10]

Government of Australia (2023), *Foreign Influence Transparency Scheme*, https://www.ag.gov.au/integrity/foreign-influence-transparency-scheme. [102]

Government of Australia - The Treasury (2022), *News Media and Digital Platforms Mandatory Bargaining Code: The Code's first year of operation*, https://treasury.gov.au/publication/p2022-343549. [79]

Government of Canada (2023), *Rapid Response Mechanism Canada: Global Affairs Canada*, https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/index.aspx?lang=eng. [111]

Government of Canada (2023), *The Online News Act*, https://laws-lois.justice.gc.ca/eng/acts/O-9.3/. [81]

Government of Canada (2021), *Security and Intelligence Threats to Elections (SITE) Task Force*, https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html (accessed on 31 August 2023). [110]

Government of France (2022), *Concentration in the media sector in the digital era: From legal rules to regulation - Executive Summary*, https://www.igf.finances.gouv.fr/files/live/sites/igf/files/contributed/IGF%20internet/2.RapportsPublics/2022/Executive_summary_anti_concentration.pdf. [44]

Government of Ireland (2022), *Report of the Future of Media Commission*, https://www.gov.ie/pdf/?file=https://assets.gov.ie/229731/2f2be30d-d987-40cd-9cfe-aaa885104bc1.pdf#page=null. [58]

Government of Norway (2016), *Act relating to transparency of media ownership*, https://lovdata.no/dokument/NLE/lov/2016-06-17-64. [47]

Government of the Netherlands (2021), *Dutch Code of Conduct Transparency Online Political Advertisements*, https://www.idea.int/sites/default/files/news/news-pdfs/Dutch-Code-of-Conduct-transparency-online-political-advertisements-EN.pdf. [7]

Government of the UK (2003), *Communications Act 2003*, https://www.legislation.gov.uk/ukpga/2003/21/section/375. [46]

GPAI (2023), *Global Partnership on Artificial Intelligence - 2023 Ministerial Declaration*, https://gpai.ai/2023-GPAI-Ministerial-Declaration.pdf. [112]

Grand Duchy of Luxembourg (2023), *Loi du 7 août 2023 portant modification: 1) du Code pénal; 2) du Code de procédure pénale*, https://legilux.public.lu/eli/etat/leg/loi/2023/08/07/a516/jo. [42]

Grand Duchy of Luxembourg (2021), *Law of 30 July on an aid scheme in favour of professional journalism*, https://legilux.public.lu/eli/etat/leg/loi/2021/07/30/a601/jo/en. [56]

International IDEA (2024), *Protecting Elections in the Face of Online Malign Threats*. [104]

International IDEA (2023), "The Information Environment Around Elections", https://www.idea.int/theme/information-communication-and-technology-electoral-processes/information-environment-around-elections. [108]

IPSOS, UNESCO (2023), *Survey on the impact of online disinformation and hate speech*. [105]

Keller, D. (2019), *Build Your Own Intermediary Liability Law: A Kit for Policy Wonks of All Ages*, Center for Internet and Society, Stanford Law School, https://cyberlaw.stanford.edu/publications/build-your-own-intermediary-liability-law-kit-policy-wonks-all-ages. [17]

Lai, S., N. Shiffman and A. Wanless (2023), *Operational Reporting By Online Services: A Proposed Framework*, https://carnegieendowment.org/files/202305-Operational_Reporting-final.pdf. [4]

Landemore, H. (2023), "Fostering More Inclusive Democracy with AI", *Finance and Development*, Vol. 60/4, pp. 12-14, https://www.scribd.com/document/689545094/What-AI-Means-for-Economics-By-IMF. [113]

Lenhart, A. (2023), *A Vision for Regulatory Harmonization to Spur International Research*, Lawfare, https://www.lawfareblog.com/vision-regulatory-harmonization-spur-international-research. [28]

Lim, G. and S. Bradshaw (2023), *Chilling Legislation: Tracking the Impact of "Fake News" Laws on Press Freedom Internationally*, Center for International Media Assistance, https://www.cima.ned.org/publication/chilling-legislation/#cima_footnote_3. [6]

Lomas, N. (2023), *Elon Musk takes Twitter out of the EU's Disinformation Code of Practice*, https://techcrunch.com/2023/05/27/elon-musk-twitter-eu-disinformation-code/. [8]

MacCarthy, M. (2021), *How online platform transparency can improve content moderation and algorithmic performance*, Brookings, https://www.brookings.edu/articles/how-online-platform-transparency-can-improve-content-moderation-and-algorithmic-performance/. [23]

Medill Local News Initiative (2023), *The State of Local News: The 2023 Report*, https://localnewsinitiative.northwestern.edu/projects/state-of-local-news/2023/report/. [40]

Meta (2023), *Changes to News Availability on our Platforms in Canada*, https://about.fb.com/news/2023/06/changes-to-news-availability-on-our-platforms-in-canada/. [82]

Nadler, J. and D. Cicilline (2020), *Investigation of Competition in Digital Markets*, https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519. [73]

Nelson, M. (2017), *What is to be done? Options for combating the menace of media capture*, Center for International Media Assistance, https://www.cima.ned.org/wp-content/uploads/2015/02/Capture12_CombatingMenace-of-Media-Capture.pdf. [43]

Newman, N. et al. (2023), *Digital News Report 2023*, Reuters Institute, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2023-06/Digital_News_Report_2023.pdf. [2]

Nielsen, R. and S. Ganter (2018), "Dealing with digital intermediaries: A case study of the relations between publishers and platforms", *Media & Society*, Vol. 20/4, https://journals.sagepub.com/doi/full/10.1177/1461444817701318. [76]

OECD (2024), *Mapping and analysis of ODA to media and the integrity of information environments*. [62]

OECD (2022), *Building Trust and Reinforcing Democracy: Preparing the Ground for Government Action*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/76972a4a-en. [3]

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, https://doi.org/10.1787/b407f99c-en. [34]

OECD (2022), "Digital enablers of the global economy: Background paper for the CDEP Ministerial meeting", *OECD Digital Economy Papers*, No. 337, OECD Publishing, Paris, https://doi.org/10.1787/f0a7baaf-en. [75]

OECD (2022), "Disinformation and Russia's war of aggression against Ukraine: Threats and governance responses", *OECD Policy Responses on the Impacts of the War in Ukraine*, OECD Publishing, Paris, https://doi.org/10.1787/37186bde-en. [91]

OECD (2022), *Handbook on Competition Policy in the Digital Age*, OECD, Paris, https://www.oecd.org/daf/competition-policy-in-the-digital-age/. [72]

OECD (2022), *The Protection and Promotion of Civic Space: Strengthening Alignment with International Standards and Guidance*, OECD Publishing, Paris, https://doi.org/10.1787/d234e975-en. [20]

OECD (2021), *Competition Issues concerning News Media and Digital Platforms*, https://web-archive.oecd.org/2021-11-19/616885-competition-issues-concerning-news-media-and-digital-platforms-2021.pdf. [77]

OECD (2021), *OECD Regulatory Policy Outlook 2021*, OECD Publishing, Paris, https://doi.org/10.1787/38b0fdb1-en. [14]

OECD (2019), *Going Digital: Shaping Policies, Improving Lives*, OECD Publishing, Paris, https://doi.org/10.1787/9789264312012-en. [71]

OECD (2019), "Recommendation of the Council on Artificial Intelligence", *OECD Legal Instruments*, OECD/LEGAL/0449, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. [114]

OECD (2014), *Accountability and Democratic Governance: Orientations and Principles for Development*, DAC Guidelines and Reference Series, OECD Publishing, Paris, https://doi.org/10.1787/9789264183636-en. [32]

OECD (2011), *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, OECD Publishing, Paris, https://doi.org/10.1787/9789264115644-en. [18]

Office of the Director of National Intelligence (2023), *2023 Annual Threat Assessment Report*, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf. [84]

Official Journal of the European Union (2022), *COUNCIL DECISION (CFSP) 2022/2478 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.LI.2022.322.01.0614.01.ENG. [96]

OSCE (2019), *The Tallinn Guidelines on National Minorities and the Media in the Digital Age*, https://www.osce.org/files/OSCE-Tallinn-guidelines-online%203.pdf. [61]

Polyakova, A. and D. Fried (2019), *Democratic defense against disinformation 2.0*. [106]

Poritz, I. (2023), *States Are Rushing to Regulate Deepfakes as AI Goes Mainstream*, https://www.bloomberg.com/news/articles/2023-06-20/deepfake-porn-political-ads-push-states-to-curb-rampant-ai-use. [117]

Quétier-Parent, S., D. Lamotte and M. Gallard (2023), *Elections & social media: the battle against disinformation and trust issues*, Ipsos – UNESCO Study on the impact of online disinformation during election campaigns, https://www.ipsos.com/en/elections-social-media-battle-against-disinformation-and-trust-issues. [1]

RSF (2023), *2023 World Press Freedom Index – journalism threatened by fake content industry*, https://rsf.org/en/2023-world-press-freedom-index-journalism-threatened-fake-content-industry. [33]

RSF (2020), *RSF's 2020 Round-up: 50 journalists killed, two-thirds in countries "at peace"*, https://rsf.org/en/news/rsfs-2020-round-50-journalists-killed-two-thirds-countries-peace. [35]

Scott, M. (2023), *I have a plan to fix social media*, https://www.politico.eu/newsletter/digital-bridge/i-have-a-plan-to-fix-social-media/. [29]

Shmon, C. and H. Pederson (2022), *Platform Liability Trends Around the Globe: From Safe Harbors to Increased Responsibility*, https://www.eff.org/deeplinks/2022/05/platform-liability-trends-around-globe-safe-harbors-increased-responsibility. [16]

Shmon, C. and H. Pederson (2022), *Platform Liability Trends Around the Globe: Recent Noteworthy Developments*, https://www.eff.org/deeplinks/2022/05/platform-liability-trends-around-globe-recent-noteworthy-developments. [15]

State of California (2018), *Senate Bill No. 1001*, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001. [12]

Sweney, M. (2023), *'The model is broken': UK's regional newspapers fight for survival in a digital world*, https://www.theguardian.com/media/2023/mar/26/regional-newspapers-fight-for-survival-in-a-digital-world. [39]

The Moscow Times (2022), *Billions for propaganda. Budget spending on state media tripled against the backdrop of the war*, https://www.moscowtimes.ru/2022/04/12/milliardi-na-propagandu-rashodi-byudzheta-na-gossmi-podskochili-vtroe-na-fone-voini-a19511. [92]

The Times of Israel (2019), *Election judge bars anonymous internet ads despite Likud objection*, https://www.timesofisrael.com/election-judge-bars-anonymous-internet-adds-despite-likud-objection/. [31]

The United States Department of Justice (2023), *Foreign Agents Registration Act*, https://www.justice.gov/nsd-fara. [99]

The United States Department of Justice (2022), *Court finds RM broadcasting must register as a foreign agent*, https://www.justice.gov/opa/pr/court-finds-rm-broadcasting-must-register-foreign-agent. [100]

The United States Department of Justice (2021), *Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System*, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere. [101]

U.S. Department of State (2023), *How the People's Republic of China Seeks to Reshape the Global Information Environment*, https://www.state.gov/gec-special-report-how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/. [95]

U.S. Department of State (2020), *GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem*, https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf. [90]

U.S. White House (2023), *Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/. [118]

UNDP (2023), *Promoting information integrity in elections*. [103]

UNESCO (2022), *Elections in Digital Times: A Guide for Electoral Practitioners*. [107]

UNESCO (2022), *Finding the funds for journalism to thrive: policy options to support media viability*, United Nations Educational, Scientific and Cultural Organization. [69]

UNESCO (2021), *UNESCO observatory of killed journalists,*, United Nations Educational, Scientific and Cultural Organization, https://en.unesco.org/themes/safety-journalists/observatory?field_journalists_date_killed_value%5Bmin%5D%5Byear%5D=2022&field_journalists_date_killed_value%5Bmax%5D%5Byear%5D=2022&field_journalists_gender_value_i18n=All&field_journalists_nationality_tid_i. [36]

United States Department of Homeland Security (2018), *Foreign Interference Taxonomy*, https://www.cisa.gov/sites/default/files/publications/foreign_interference_taxonomy_october_15.pdf. [86]

United States Department of Justice (2022), *Recent FARA Cases*, https://www.justice.gov/nsd-fara/recent-cases. [38]

United States Department of State (2022), *Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propoaganda Ecosystem*, https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf. [93]

USAID (2023), *Administrator Samantha Power Delivers Remarks at the "Advancing Technology for Democracy" Event*, https://www.usaid.gov/news-information/speeches/mar-30-2023-administrator-samantha-power-delivers-remarks-at-the-advancing-technology-for-democracy-event. [67]

USAID (2023), *Interventions to Counter Misinformation: Lessons from the Global North and Applications to the Global South*, https://pdf.usaid.gov/pdf_docs/PA0215JW.pdf. [68]

Vilmer, J. (2019), *The "Macron Leaks" Operation: A Post-Mortem*. [97]

NOTES

[1] For additional information, see: https://santaclaraprinciples.org/.

[2] For additional information, see: https://c2pa.org/.

[3] For additional information, see: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

[4] Information provided by the Government of Lithuania.

[5] For additional information, see: https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180. Note that draft Bill 2630/2020 seeks to update the Marco Civil da Internet by, in part, including a "duty-of-care" for digital platforms to take action on specific illegal content.

[6] For additional information, see: https://www.infrastructure.gov.au/have-your-say/new-acma-powers-combat-misinformation-and-disinformation.

[7] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2002:201:FULL.

[8] See of S.1989 – Honest Ads Act Section 8(4)(ii) (https://www.congress.gov/bill/115th-congress/senate-bill/1989/text) and Proposal for a Regulation of the European Parliament and of the Council on the Transparency and Targeting of Political Advertising Article 2(2)(b) (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0731).

[9] For additional information, see: https://fom.coe.int/en/accueil.

[10] For additional information, see: https://www.mfrr.eu/monitor/.

[11] For additional information, see: https://www.coe.int/en/web/freedom-expression/safety-of-journalists-campaign

[12] For additional information, see: https://cmpf.eui.eu/media-pluralism-monitor-2023/.

[13] Countries in the study included: Austria; Belgium; Bulgaria; Croatia; Cyprus; Czechia; Denmark; Estonia; Finland; France; Germany; Greece; Hungary; Ireland; Italy; Latvia; Lithuania; Luxembourg; Malta; The Netherlands; Poland; Portugal; Republic of North Macedonia; Romania; Serbia; Slovak Republic; Slovenia; Spain; Sweden; Türkiye; United Kingdom.

[14] For additional information, see: https://lovdata.no/dokument/NLE/lov/2020-05-29-59.

[15] For more information on background and recommendations related to improving the policy, funding, and enabling environment for independent professional journalism, see: (Forum on Information and Democracy, 2021[54]).

[16] Such as the requirement in Luxembourg that the public service media must be organised in a way that "ensures autonomy and independence from the State and social, economic and political entities with regard to editorial decisions" – see Luxembourg's *Law of 12 August 2022 on the organisation of the public establishment 'Public Service Media 100,7' and amending the amended Law of 27 July 1991 on electronic media* for additional information.

[17] For additional information, see: https://freedomonlinecoalition.com/donor-principles-for-human-rights-in-the-digital-age/.

[18] For additional information, see: https://ifpim.org/.

[19] For text of the legislation, see: https://www.legislation.gov.au/Details/C2019C00133.

[20] Generative AI refers to artificial intelligence systems capable of generating text, images, or other media in response to prompts.

3 Fostering societal resilience to disinformation

This chapter presents policies and practices for a multi-stakeholder approach to information integrity. It discusses efforts to help provide the public with the skills to navigate the evolving information environment with a discerning view and critical approach and help facilitate the search for consensus through media and information literacy and the necessary evolution of the role of public communication. The chapter also explores the importance of strengthening participatory measures to inform the policy-making process in this space.

3.1. INTRODUCTION

Countering disinformation and strengthening information integrity require concerted efforts to build societal resilience. Broadly, resilience is about addressing the root causes of crises while strengthening the capacities and resources of a system to cope with risks, stresses, and shocks (OECD, 2023[1]). Applied to tackling disinformation and strengthening information integrity, resilience refers to a society's ability to understand, resist and recover from threats within the information space. Indeed, several countries have situated societal resilience to information threats as part of building a comprehensive or total defence system, in which every individual and organisation should play a role, including as checks and balances in the overall information ecosystem.

On the one hand, therefore, individuals need skills and knowledge to navigate the information space effectively and responsibly. Government investments in digital, media and information literacy – and efforts to help ensure private companies actively contribute to societal resilience efforts – are important means to prepare and inoculate people against false and misleading content. According to PISA (Programme for International Student Assessment) results, in 2018 only 47% of 15-year-old students across OECD countries reported that they were taught how to detect whether information is subjective or biased at school (OECD, 2021[2]). A person that can navigate the information space responsibly will likely be more able to assess critically the content they encounter, to find higher-quality sources, to identify biases, and make well-informed decisions.

Furthermore, developing a public communication function removed from politicised goals to serve as a source for accurate and relevant information, and that is responsive to citizens in the service of the common good, is an important tool to build societal resilience. More broadly, the value of access to information as a key safeguard for democracy has become more evident in the past years. Various crises, ranging from financial to health to defence, have increased the need and demand for accurate information from government itself (OECD, 2022[3]).

At the same time, fostering resilience to disinformation will require governments to strengthen public engagement mechanisms on topics related to information integrity as part of the larger undertaking to reinforce democracy and build trust. Engagement with the public and non-governmental stakeholders should ultimately be guided by efforts to protect and strengthen civic space to foster more open, transparent, and accountable governance (OECD, 2022[3]). Expanding research and understanding of the information space (namely, the convergence of the public, communication technologies, amplification algorithms, and content), and ensuring the findings inform the policymaking process, will also be essential contributions (Wanless and Shapiro, 2022[4]). Governments should therefore focus on expanding the competencies, resources, and reach of efforts in this space to facilitate participation and understanding across all segments of society.

Together, these efforts compose what is often referred to as a whole-of-society approach. That said, an effective whole-of-society approach also requires protecting the human rights of those targeted by disinformation. It also requires promoting civic education, as well as clarifying processes, expected outcomes, and mechanisms both to mitigate potential risks and to take full advantage of the opportunities to engage with the public and non-governmental stakeholders. For example, the Netherlands' 2022 government-wide strategy for effectively tackling disinformation explicitly mentions the role of civil society and academics in fighting disinformation (Government of Netherlands, 2022[5]). Similarly, the 2023 Latvian counter-disinformation programme stresses the importance of government co-operation with stakeholders across society. The 2022 updated EU Code of Practice on Disinformation, furthermore, defines stronger and formalised roles for the fact-checking community, and the EU Digital Services Act creates obligations for online platforms and search engines to co-operate with fact checkers in the framework of Code of Practice (European Union, 2022[6]).

To reinforce societal resilience against the risks of mis- and disinformation and implement a whole-of-society approach, government efforts should focus on:

- Strengthening media, information, and digital literacy skills
- Helping ensure the public is well informed via proactive and public communication efforts removed from politicised goals, and

- Strengthening public participation in information integrity efforts and building understanding of the information space.

3.2. MEDIA, INFORMATION, AND DIGITAL LITERACY IS ESSENTIAL TO DEVELOPING A SYSTEMIC APPROACH TO BUILDING SOCIETAL RESILIENCE

A long-term and systemic effort to building societal resilience to the challenges posed by disinformation involves building media, digital, and information literacy to help ensure the public can participate in the information environment with a discerning view and critical approach. There are several definitions of what media, digital, and information literacy includes. For example, the EU's Audiovisual Media Services Directive (AVMSD) stipulates that media literacy refers to skills, knowledge and understanding that allow citizens to use media effectively and safely. Beyond learning about specific tools, technologies, and threats, media literacy more broadly aims to equip individuals with the critical thinking skills required to exercise judgment, analyse complex realities, and recognise the difference between opinion and fact (European Union, 2018[7]). The UK's independent communications regulator, Ofcom, defines media literacy as "the ability to use, understand and create media and communications in a variety of contexts" (Ofcom, 2023[8]). UNESCO defines media and information literacy (MIL) as an effort to: "Empower people to think critically about information and use of digital tools. It helps people make informed choices about how they participate in peace building, equality, freedom of expression, dialogue, access to information, and sustainable development (UNESCO, 2023[9])." Digital literacy, furthermore, focuses on the competencies needed to live and work in a society where communication and access to information increasingly takes place through digital technologies (OECD, 2022[10]).

A comprehensive understanding of media, information, and digital literacy focuses on the public's skills related to accessing, analysing, evaluating, and creating content in a variety of contexts (Hill, 2022[11]). This range of skills includes both understanding the creation and distribution process, as well as developing the ability to take a critical approach to evaluating information reliability. Governments largely recognise the importance of building media and information literacy skills. Within Europe, the EU's Audiovisual Media Services Directive (AVMSD) (European Union, 2018[7]), which governs EU-wide co-ordination of national legislation on all audio-visual media, includes specific provisions requiring Member States to promote media literacy skills and to report on these actions, and obliges media service providers and video-sharing platforms to promote the development of media literacy and raise awareness of available media and digital literacy tools (European Commission, 2023[12]). The European Regulators Group for Audiovisual Media Services, furthermore, is tasked with exchanging experience and best practices on the application of the regulatory framework for audiovisual media services, including on accessibility and media literacy. As of 2022, in the United States, 18 states have passed legislation requiring education agencies to develop and include media literacy curricula in schools (Media literacy now, 2022[13]).

Taken together, governments should prioritise the following elements when considering how media and information literacy initiatives best fit into broader efforts to build societal resilience:

- Media and information literacy initiatives should be seen as part of a wider effort to reinforce information integrity, including by incorporating such efforts into official curricula and reaching individuals of all ages in relevant efforts
- Pro-active public communication efforts, or "pre-bunking," can be useful media and information literacy tools to help build societal resilience
- Assessing and measuring impact of media and information literacy activities.

3.2.1. Media and information literacy initiatives should be seen as part of a wider effort to reinforce information integrity

The aim of the media, information, and digital literacy initiatives largely focuses on efforts to give people the tools to make conscious choices online, identify what is trustworthy, and understand platforms' systems in order to use them for their own benefit (Forum on Information and Democracy, 2023[14]). Media and information

literacy should be part of a larger approach to building digital literacy, for example by focusing on elements related to addressing how algorithm recommendation systems and generative AI work, as well as civic education, for example by teaching the importance of democratic principles and processes and focusing both on school-aged individuals, as well as adults and seniors.

Ultimately, media literacy initiatives are most relevant to the extent that they reinforce broader objectives related to strengthening information integrity. For example, Portugal's National Plan for Media Literacy highlights that media literacy is a fundamental element for the defence of freedom of expression and information, and is essential to enabling democratic participation and the "realisation of economic, social, cultural and environmental rights (Government of Portugal, 2017[15])." A notable component of Finland's approach, furthermore, is that their focus on media literacy has long been perceived as part of a wider effort to build societal resilience to disinformation. Media education initiatives have been present in Finnish schools since the 1950s, and the country has focused its media education efforts on promoting people's willingness and ability to consume, use and share information in a responsible way, and, ultimately, contribute to citizens' active participation in society (see Box 3.1).

Box 3.1. Media literacy in Finland

Finland's approach to media literacy is outlined in the National Media Education Policy, published by the Ministry of Education and Culture in 2019, in collaboration with the National Audiovisual Institute (KAVI). The promotion of media literacy is a cross-cutting activity for the Ministry of Education and Culture and has expanded to cover other areas of society and administration.

The 2019 National Media Education Policy in continues a decades-long effort to promote democratic participation and reduce polarisation in Finnish society. While the first media education curriculum was introduced in Finnish schools in 2004 through an action plan addressing violence in the media and media education, media education initiatives have been present in Finnish schools since the 1950s.

Today, the concepts of misinformation and disinformation are part of student coursework, including the study of famous propaganda campaigns, advertising, and tactics for using misleading statistics. As part of the curriculum, students create their own messages and multi-media products on different topics to share with their peers for comment and analysis.

Finnish media education involves a range of actors in developing media education plans, including civil society organisations, schools, libraries, NGOs and universities. Finland also promotes media literacy following European Union guidance, such as the Audiovisual Media Services Directive (EU 2018/1808) and the Communication from the Commission on Tackling Online Disinformation. The National Audiovisual Institute, in co-operation with the Ministry of Education and Culture, is responsible for evaluating the implementation of the action plan.

Source: Government of Finland (2019[16]), *Media Literacy in Finland: National Media Education Policy*, Ministry of Education and Culture, https://medialukutaitosuomessa.fi/mediaeducationpolicy.pdf.

In some OECD Member countries, media and information literacy is centrally co-ordinated, for example by the National Audio-visual Institute, KAVI, in Finland; the *Centre de liaison de l'enseignement et des médias d'information,* CLEMI, in France (see Box 3.2); or the National Media Regulatory Authority (ALIA) in Luxembourg, which co-ordinates media literacy activities with relevant national and European stakeholders. In Portugal, the Regulatory Authority for the Media has helped facilitate media literacy by mapping the range of existing interventions to promote and develop this space in the country (Portuguese Regulatory Authority for the Media, 2023[17]). In other countries, the responsibilities are spread across different institutions, such as ministries of education, other line ministries or national regulatory authorities.

The most common approach is for countries to provide media literacy within schools (see the example from Estonia in Box 3.3), either via a separate curriculum specifically devoted to media and information literacy or included within other topics (for example, language, mathematics, history, citizenship). In Portugal, for example, the curriculum integrates media literacy via citizenship and information and communication technology sections. The country's Guidelines for Media Education (*Referencial para a Educação para os Media*), updated in December 2023, underline that media literacy is interdisciplinary and should be reinforced across learning areas, as well through projects with the National Network of School Libraries and with external organisations.

Box 3.2. The "CLEMI": France's centre to promote and co-ordinate media and information literacy activities

In France, the CLEMI (*Le centre pour l'éducation aux médias et à l'information*) is in charge of media and information literacy throughout the French education system. The CLEMI was created in 1983 its mission is to promote, both nationally and in France's "académies", the pluralistic use of information tools in education to foster a better understanding by students of the world around them while developing their critical thinking skills.

Its objectives are the following:

- Training teachers and teaching pupils how to use media responsibly, whatever the information or communication medium (written press, audiovisual, Internet, social networks).
- Producing or co-producing teaching resources and tools on all media to support teachers and pupils by offering MIL activities for the classroom.
- Helping to create and develop school media (newspapers, websites, blogs, web radio, web TV).
- Supporting families by producing and distributing media and information education tools for all.

Since the official text of January 24, 2022 (*circulaire du 24-1-2022*), regarding the mainstreaming of media and information literacy (MIL) in France, the CLEMI collaborates closely with the French Ministry of Education and Youth. Together, they oversee a network of 30 academic focal points, each tasked with leading cells that unite all inspection bodies and academic delegations. CLEMI's initiatives are supported by a national team of 22 individuals, a network of 200 local academic co-ordinators, and numerous media partners, all contributing to the development of projects for schools.

Source: CLEMI (n.d.[18]), CLEMI website, https://www.clemi.fr/fr/qui-sommes-nous.html.

Box 3.3. Estonia's "Media and Manipulation" course in the high-school curriculum

Since 2010, Estonia has included a compulsory "Media and Manipulation" course in the high school curriculum. The goals of the 35 academic hour course are that, by the end of it, students can:

- Understand the modern information environment and the processes that shape its development and explain the nature of communication and the conditions for its occurrence.
- Identify arguments and basic persuasion techniques in media texts and explain the author's objectives and motives.
- Distinguish between facts and opinions, assess the reliability of information, including changes in the meaning of translated information.
- Critically analyse advertising and discuss advertising and branding topics.
- Understand media channels, analyse their characteristics, and describe different media genres.
- Analyse the differences between direct and mediated communication and the intentions of participants.
- Critically evaluate media manipulation, recognise propaganda, fake news, and myth making.
- Express their opinion on what they have read, heard, and seen and choose appropriate language tools for this purpose.
- Critically analyse their media behaviour, including on social media, and adjust it accordingly to the situation.
- Find references and clues to other texts, interpret text, and distinguish between private and public information.

Source: Data provided by the Estonian government.

OECD countries also produce manuals and guidebooks on understanding and counteracting the threat of mis- and disinformation. These are distributed on official websites and in print, to be shared with schools and public libraries. For example, in 2022, the Latvian State Chancellery published a digital book entitled "Handbook against disinformation: recognise and oppose" (*Rokasgrāmata pret dezinformāciju: atpazīt un pretoties*)[1]. The manual summarises practical recommendations for state administration and local government workers, as well as all Latvian residents, to address information manipulation. The manual is distributed to libraries throughout the country. The Ministry of Interior in the Netherlands, for its part, finances the creation and operations of the website "Is that really so?",[2] which teaches the population how to identify mis- and disinformation.

Media and information literacy activities are often developed and implemented in partnership with a wide range of civil society organisations. The tendency toward this whole-of-society approach is borne out by the amount of CSOs, media and other organisations working in this field. For example, the United Kingdom identified at least 175 organisations focused on media literacy and in Finland, KAVI has identified almost 100 organisations promoting media literacy. For its part, the Norwegian Media Authority has established a media literacy network to provide a forum for organisations representing researchers, businesses, civil society organisations and governmental bodies to share information and identify priority issues to address. In the Netherlands, furthermore, the Dutch Media Literacy Network connects close to 1 000 non-governmental organisations (see Box 3.4).

Box 3.4. Dutch Media Literacy Network

The Ministry of Education, Culture and Science established the Media Literacy Network in 2008, and it currently has over 1 000 organisations as members, including public libraries, cultural institutions, education publishers and welfare organisations.

The Ministry funds the network's programme activity plan. The network's core partners deliver up-to-date media literacy programmes and support members' activities through a 'coordinating core' of five committees and groups. The partners provide independent advice on developments in media literacy; conduct research; oversee staffing and funding; manage relations with the network; and perform evaluation tasks through satisfaction surveys of network members. The network's accomplishments are traced through its press page, which also publishes statements, briefs, and research related to media literacy.

In addition to media literacy programmes, the Network increases awareness of media literacy and shares knowledge, expertise, and resources through its online resources. For example, Netwerkmediawijsheid.nl is the main online platform for the Network's partners and other professionals working in media literacy. Mediawijsheid.nl hosts resources for school leaders and boards to permanently integrate media literacy into school education. HoeZoMediawijs.nl is a resource aimed at children older than 10 focused on protecting oneself online, information and games about using social media, and judging the reliability of information, among others.

Source: The Dutch Media Literacy Network (n.d.[19]), "About Dutch Media Literacy Network", https://netwerkmediawijsheid.nl/over-ons/about-dutch-media-literacy-network/.

Governments also often partner with non-government organisations to provide media literacy initiatives, where CSOs and governments work together to prepare campaigns, informational and study materials, gamified solutions, and training videos. In Norway, the campaign "*Stopp.Tenk.Sjekk*" (Stop, Think, Check) was developed before the 2021 elections and is a co-operation between the Norwegian Media Authority and the fact-checking service Faktisk.no, the National Association of Local Newspapers, the Norwegian Directorate for Civil Protection (DSB), and with support from Meta. The campaign recommends six questions for individuals to ask themselves when reading content online, with the aim of helping people think critically about whether an article, post, or piece of news is trustworthy. A new version of the campaign was created concerning Ukraine in 2022, as well as prior to the 2023 elections (Norwegian Media Authority, 2021[20]). Similarly, the Be Media Smart campaign in Ireland flags the importance of knowing how to verify information, provides tips and guidance on how to check the accuracy and reliability of information, and provides information on sources of support and training (see Box 3.5).

Box 3.5. Ireland's "Be Media Smart" media literacy campaign

An initiative of Media Literacy Ireland (MLI), a largely voluntary informal network of individuals and organisations that promotes media literacy in Ireland, the "Be Media Smart" campaign encourages people to Stop, Think, and Check that the information they read, see, or hear is reliable and accurate.

First launched in 2019 as part of a European initiative to counter disinformation in advance of the 2019 European elections, the campaign evolved in 2020 to focus on accurate and reliable information about COVID-19. In 2021, the focus was on helping individuals make informed choices about the COVID-19 vaccination based on accurate and reliable information. The message was delivered in Irish and English across TV, radio, and news publications across community, commercial, public service, and social media platforms.

All TV and radio advertisements were produced, distributed, and broadcast free-of-charge by MLI members from the media sector with added visibility provided by editorials highlighting the initiative. A co-ordinated social media campaign with a diverse range of MLI members using freely available social media assets also boosted the campaign and the call to action. All Be Media Smart communication directed people to the Be Media Smart website (available in Irish and English) for advice and support, a FactCheck section, and an 'Ask an Expert' section, where members of the public can put media literacy related questions to a panel of experts.

In 2023, the "Be Media Smart" campaign incorporated a Be Media Smart Community Training Programme. The training programme, developed in conjunction with EDMO Ireland, trained over 100 community-based leaders, coaches, and librarians to use the Be Media Smart Workshop in a Box resource to deliver media literacy training in English and in Irish in their own communities.

Research carried out by Ipsos B&A in November 2023 noted that 23% of adults recalled the campaign, unprompted, compared to the 15% before the media campaign started (for context, recall rates of between 13%-17% is considered successful for similar campaigns). In addition, 45% of respondents to the survey in December 2023 said that they would take action if they came across information that was false or misleading, compared to 32% in April 2021.

Facilitated by the newly established media regulator in Ireland, *Coimisiún na Meán*, and supported by media, civil society organisations, libraries, educational, training and research institutions and search and social platforms, this project shows the power of collaboration and the benefits that can be achieved when organisations collaborate to contribute ideas and skills. The European Platform of Regulatory Authorities (EPRA) and EDMO have highlighted the campaign as a best practice example, and the concept and elements of the campaign have been adopted in at least four other European countries.

Source: Government of Ireland; Media Literacy Ireland (n.d.[21]), "What is Media Literacy Ireland?", https://www.medialiteracyireland.ie/;
Be media smart (2023[22]), Be media smart website, https://www.bemediasmart.ie/.

Another co-operation format is "media literacy weeks", such as those organised by UNESCO, across the European Union, and in several countries. In Finland, for example, every year around 30 different materials or campaigns are created in co-operation with more than 50 partner organisations from all sectors of society, including public institutions, NGOs, and private companies (Media Literacy Week, 2023[23]).

Media and information literacy activities may also include efforts to better understand and reach groups susceptible to mis- and disinformation, but that are not reached by more traditional initiatives, such as older populations, diasporas and second-language communities, socioeconomically disadvantaged groups, people with disabilities, and migrants. For their part, older populations often have weaker digital skills and are more prone to sharing mis- and disinformation compared to younger cohorts of the population (Guess, Nagler and Tucker, 2019[24]). Efforts to reach these group include projects devoted to media literacy of retired people through seniors' centres, public libraries, and other community settings. For example, the Norwegian Media Authority worked with the non-governmental organisation Seniornet to develop educational resources for seniors, including printed booklets, presentations, and in-person meetings that build media and digital literacy within that population.

Other vulnerable groups that media and information literacy activities target include diasporas and second-language communities. To that end, Baltic states have designed specific media literacy campaigns to reach Russian speakers, such as the Latvian government's project it has carried out with the CSO Baltic Centre for Media Excellence. In addition to working through schools, therefore, governments should identify approaches to expand media and information literacy activities to particular groups of the population that traditional programmes might not otherwise reach (see Box 3.6 for examples from the United Kingdom).

Box 3.6. United Kingdom efforts to help vulnerable people to spot disinformation and boost online safety

The United Kingdom has funded projects with 17 organisations to pilot new ways of boosting media literacy skills for people at risk of experiencing online abuse and being deceived into believing false information, such as vaccine disinformation, deepfake videos or propaganda created by hostile states.

The Media Literacy Taskforce Fund is one of two funding schemes created to target 'hard-to-reach' and vulnerable groups by investing in community-led projects to ensure everyone can improve their media literacy skills and protect themselves from online disinformation through:

- A social enterprise working with young people to develop their own podcasts exploring online mis- and disinformation to be aired on local radio
- A project run by a charity to provide media literacy training focused on care workers
- Access to digital media skills training online and in community centres for the elderly
- A partnership with NewsGuard and charities that delivers workshops to older adults to support them in spotting mis- and disinformation online
- The Economist Educational Foundation, to work with disadvantaged schools and boost teachers' skills through news literacy training and support students to engage with the news and think critically about what they're consuming online
- The online safety charity Glitch, which will deliver workshops and training to vulnerable and marginalised women to support their media literacy skills including tackling online abuse.

Source: Government of the UK (2022[25]), "Help for vulnerable people to spot disinformation and boost online safety", https://www.gov.uk/government/news/help-for-vulnerable-people-to-spot-disinformation-and-boost-online-safety.

3.2.2. Pro-active pre-bunking communication efforts can help build societal resilience to the spread of disinformation

Governments can also help prepare society to better understand disinformation flows and risks by "inoculating" the public to the potential harms. These "pre-bunking" efforts seek to "warn people of the possibility of being exposed to manipulative disinformation, combined with training them on how to counter-argue if they do encounter it," with the idea that such activities will reduce their susceptibility to false and misleading content (Roozenbeek and van der Linden, 2021[26]) (Van der Linden, 2023[27]). Pre-bunking and other pro-active communication efforts can focus on flagging disinformation actors, sources of inauthentic information, and on assessments and insight into tactics used to create and share misleading content (OECD, 2023[28]).

To this end, governments have created and distributed materials and organised internet campaigns that inform the public about the dangers of mis- and disinformation, name-and-shame malign actors, and share examples of how information attacks and false narratives can spread. Lithuania, Latvia, Estonia, Finland, Czechia, and others, notably through their intelligence agencies have in recent years started to publicly disseminate analytical reports and threat assessments. These often devote considerable attention to the information environment, including malign actors, examples of relevant attacks and manipulations, and target audiences. Such reports provide the public with reliable information on the major threats (see Box 3.7).

Box 3.7. Security and Intelligence assessments – Case studies from Lithuania, Latvia, Finland and Sweden

Intelligence and security agencies in some OECD members have published public threat assessments or reports as a means of keeping policymakers and the public informed of relevant issues. Finland's Security and Intelligence Service (SUPO) has produced reports since 2016, Latvia's State Security Service since 2013, Lithuania's Second Investigation Department under the Ministry of National Defence and State Security Department since 2014, and Sweden' Security Police since 2001.

Finland, Latvia, Lithuania, and Sweden each produce annual reports that contain updates on malign information campaigns and strategies within the context of broader threats facing the country. Recent editions have highlighted the disinformation campaigns related to Russia's war of aggression against Ukraine, which primarily seek to sway opinion in support of Russia's invasion and justify its actions by taking advantage of perceived social tensions in the region.

Latvia's latest report identifies long-term exposure to disinformation and propaganda, low levels of education, and the influence of "opinion leaders" as exacerbating the effect of malign information campaigns. Lithuania's report also identifies personalities with links to Russia or Belarus as instigating disinformation. Similarly, it outlines how social issues, such as the 2020 migration crisis manufactured by Belarus, play a central role in Russian and Belarusian disinformation campaigns.

In a similar vein, Sweden's report describes disinformation as a key factor in attempts to destabilise or undermine society and the democratic state. Narratives to this end portray Sweden as a country in "chaos and decay", with COVID-19 described as a watershed moment for the spread of hate and distrust in society through malign information and conspiracy theories. Finland's SUPO report also underscores outsider efforts to influence security policy decisions by preventing open discussions, such attempts to influence public debates around NATO membership as a direct threat to national security.

The reports show that the methods and vulnerabilities malign actors exploit are similar. Detailing the messages, narratives, and techniques for spreading malign information allows readers to more effectively identify and react to potential threats.

Source: Supo (2022[29]), "Supo Yearbook 2021: Finns must be prepared for influencing efforts from Russia during NATO debate", https://supo.fi/en/-/supo-yearbook-2021-finns-must-be-prepared-for-influencing-efforts-from-russia-during-nato-debate; Latvian State Security Service (n.d.[30]), Annual reports, https://vdd.gov.lv/en/useful/annual-reports; Republic of Lithuania (2022[31]), *National Threat Assessment 2022*, https://www.vsd.lt/wp-content/uploads/2022/04/ANGL-el- .pdfv; Swedish Security Service (n.d.[32]), Sweden Security Police Yearbooks, https://www.sakerhetspolisen.se/om-sakerhetspolisen/publikationer/sakerhetspolisens-arsberattelse.htm.

Based on these assessments, governments have also organised special courses for representatives of civil society, media, academics, business on national security and defence topics. The content of these courses includes information on threats, as well as opportunities to discuss the issues with government officials. Such efforts support societal resilience by raising participants' awareness of threats and preparing them for co-operation in the case of a crisis. Beyond raising awareness, the benefits of such endeavours help participants serve as ambassadors to spread the understanding and skills to members of their respective organisations and the public.

Another practical example of a public and accessible pre-bunking tool is the development of the GoViral! Game, created by a collaboration between academic researchers, the UK Cabinet Office, the World Health Organisation and three private sector design agencies. The game exposes players to manipulation techniques and simulates real-world social media dynamics to share insights into of how mis- and disinformation are spread (see Box 3.8). A strength of these pre-bunking efforts is that while they inform the public of actual disinformation threats and techniques, they do not put governments in the position of discussing specific pieces of content or serving as an arbiter of truth.

Box 3.8. GoViral! Pre-bunking game

Funded by the UK Cabinet Office and supported by the UN World Health Organisation, Go Viral! was created by researchers from the University of Cambridge Social Decision-Making Laboratory and the Sciences Po Médialab. The game was built with the help of design agencies and builds on previous research showing that a similar game simulating the spread of disinformation, Bad News, can reduce susceptibility to false information for at least three months.

Launched in October 2020, the five-minute game exposes players to three common manipulation techniques used in spreading COVID-19 mis- and disinformation: emotional language, fake experts, and conspiracy theories. It aims to demystify and pre-bunk false information by simulating a real-world social media environment.

Within the game, players create a viral social media post using emotionally evocative language, share content using fake experts to gain credibility in a social media group, and create their own COVID-19 conspiracy theory, targeting an entity or organisation to spark protests. The game allows players to assess the popularity and perceived trustworthiness of their content, simulating the dynamics of real-world social media interactions.

At the start of gameplay, players are invited to take part in research questions about how they perceive certain pieces of content. They are then asked similar questions at the end. Analysis of the results found that the game increases perceived understanding of misinformation about COVID-19, improves confidence in the ability to spot false and misleading content, and reduces self-reported willingness to share such content with others.

The Go Viral! Game shows how collaboration between governments, international organisations, and academic institutions can inform cutting edge research into societal challenges. The ability to gather data throughout the game is also an effective way to measure the game's effectiveness and gather user feedback.

Source: www.goviralgame.com; Maertens et al. (2021[33]), "Long-term effectiveness of inoculation against misinformation: Three longitudinal experiments", *Journal of Experimental Psychology: Applied*, Vol. 27/1, pp.1–16, https://doi.org/10.1037/xap0000315; Basol et al. (2021[34]), "Towards psychological herd immunity: Cross-cultural evidence for two prebunking interventions against COVID-19 misinformation", *Big Data & Society*, Vol. 8/1, https://doi.org/10.1177/20539517211013868.

3.2.3. Continued focus should be given to assessing and measuring impact of media and information literacy activities

Despite the general agreement on the necessity and value of providing media and information literacy skills, several challenges exist. First, the effectiveness of media literacy activities is heavily dependent on the capacity of teachers and trainers, as well as the quality of available materials. One way to help ensure consistent implementation of MIL activities, therefore, is for countries to establish a system of teacher training. Notably, the French centre "CLEMI" trains around 17 000 teachers on media and information literacy each year (CLEMI, 2023[35]). The consistency of training through the school system may also be hindered in countries with less centralised education system. Such systems may also enable greater innovation and experimentation, though it can lead to variable quality between approaches.

Attention should also be given to the quality of partners conducting MIL activities that are funded in whole or in part by the state. Given the range of potential actors, quality control, monitoring, and cost / benefit assessments are essential, despite adding administrative costs. Particularly where partners are providing media literacy campaigns, governments should put in place effective mechanisms to ensure the content, methods, and quality of products fit general requirements and that the activities align with strategic goals.

Another challenge that all MIL efforts face is related to difficulties in assessing and measuring impact of the activities. Formal measurement criteria usually involve obligations to report on outputs, such as a list of the events or other activities, the audience reached (for example, views on the website or social platform or the number of the participants in events), hours spent in trainings, and mentions of the project in the other media sources. Even if output measurements exist, such criteria do not often illustrate the actual impact of the project on its intended goals or broader changes over time in the capacity for critical and reflective information consumption. Without careful assessment, it is not clear how activities practically change participants' attitudes or whether the effect is long-lasting. This challenge is magnified in less formal settings, where participation is not mandatory and may be less consistent.

Such issues point to the need for clear methodology for evaluating the effectiveness of MIL activities. The Council of Europe analysed 68 MIL projects in 2021 in the field of media literacy and found that one third of the projects did not include any measurement parameters (Council of Europe, 2016[36]). In the United Kingdom, the national online media literacy strategy explicitly stipulates the need for better measurement in this field. The analysis noted a "distinct lack of robust evaluation of media literacy provisions." Where evaluation measures exist, they are often very limited, using metrics such as reach, number of events, quotes from participants, or participant self-assessments, making it challenging to assess whether provisions are effective at improving media literacy capabilities on a long-term basis (UK Department for Digital, Culture, Media & Sport, 2021[37]).

Media literacy providers, furthermore, often do not have sufficient funding to be able to monitor and evaluate their initiatives. Relatedly, interventions also often operate on a short-term basis and do not facilitate working with the same beneficiaries over a long enough time frame to determine the effectiveness of the activities. To that end, many aspects of media literacy that are cemented in behavioural change can be difficult or impossible to measure over the short-term; for example, assessing whether users are able to independently apply learnings to the 'real' online environment, rather than just under supervision (UK Department for Digital, Culture, Media & Sport, 2021[37]).

For its part, the Norwegian Media Authority conducts an assessment every two years on the state of the media literacy in the country. The latest report was published in 2021 and is based on the representative opinion poll of 2048 Norwegian residents. Among its findings are that the oldest (aged 60+) and youngest (aged 16–24) segments of the population find it most difficult to deal with disinformation, and that while 50% of the population reports that they check other sources they trust to verify information, 18% note that they do not verify information at all (Norwegian Media Authority, 2021[38]). (see Box 3.9 for additional examples of media literacy assessment tools).

Box 3.9. Media literacy assessment tools

UK Ofcom toolkit for evaluating media literacy interventions

The Making Sense of Media programme within the UK telecommunication regulator Ofcom published a toolkit in 2023 to help guide evaluations of media literacy interventions. The toolkit, which provides a series of how-to guides for planning and carrying out an evaluation of media literacy interventions, is an important element of Ofcom's programme of work supporting the media literacy in the United Kingdom.

The toolkit gives practical and straightforward guidance and advocates for an evaluation process that is part of the project from the start. It explains that evaluation *proves* (in that an initiative has achieved its desired outcomes) and *improves* (in that the initiative provides insights and learnings for an organisation). The Toolkit also details the importance of demonstrating impact – notably, change at an individual or societal level that can be attributed to a project – and takes organisations through steps to help them show evidence.

The Toolkit is divided into three sections that represent stages in the evaluation process: Preparing; Doing; and Sharing. First, it discusses how to write a theory of change and how to create an evaluation framework. Second, it provides information about research methods and proposes model questions; the third section suggests how organisations can structure evaluation reports. There is a separate evaluation framework template, as well as searchable libraries that help map media literacy research and media literacy initiatives within the United Kingdom.

European Union DIGCOMP framework

The Digital Competence Framework for Citizens, also known as DigComp, provides a common language to identify and describe the key areas of digital competence. It is an EU-wide tool designed to improve individuals' digital competence, help policymakers formulate policies and initiatives, and plan education and training initiatives to improve the digital competence of specific target groups. In this way, digital competence involves the "confident, critical and responsible use of, and engagement with, digital technologies for learning, at work, and for participation in society."

The DigComp framework identifies the key components of digital competence in 5 areas:

- Information and data literacy seeks to ensure the public can articulate information needs, locate and retrieve digital data, information and content, as well as judge the relevance of data sources and content.
- Communication and collaboration seeks to ensure the public can interact, communicate and collaborate through digital technologies while being aware of cultural and generational diversity; participate in society through public and private digital services and participatory citizenship; and manage one's digital presence, identity, and reputation.
- Digital content creation focuses on skills related to creating and editing digital content.
- Safety focuses on protecting devices, content, personal data and privacy in digital environments and protecting physical and psychological health.
- Problem solving focuses on ensuring the public can identify needs and problems and use digital tools to innovate processes and products to keep up-to-date with the digital evolution.

Source: Ofcom (2023[39]), *A toolkit for evaluating media literacy interventions*, https://www.ofcom.org.uk/research-and-data/media-literacy-research/approach/evaluate/toolkit; Morris (2023[40]), Ofcom's Toolkit for Evaluating Media Literacy Interventions, https://media-and-learning.eu/type/featured-articles/ofcoms-toolkit-for-evaluating-media-literacy-interventions/; European Commission (n.d.[41]), "DigComp", https://joint-research-centre.ec.europa.eu/digcomp_en.

The challenges related to the costs, processes, and independence of assessing media, information, and digital literacy initiatives point to the opportunity provided by working with external partners and experts to provide independent perspectives. For example, the U.S. Department of State GEC supported the development of two web browser-based media and information literacy games. The University of Cambridge Social Decision-Making Lab independently assessed the efficacy of both games, which has enables the GEC to monitor the games' efficacy and continue to make changes (Box 3.10).

Box 3.10. Harmony Square and Cat Park media and information literacy games

The U.S. Department of State's Global Engagement Center (GEC) developed two measurably effective media and information literacy games to build resilience to foreign information manipulation and influence overseas: Harmony Square and Cat Park.

Harmony Square launched in November 2020 and is currently available in 18 languages. The game is intentionally apolitical (notably, the player attacks topics such as pineapple on pizza and a fictional election for bear patroller). Taking on the role of Chief Disinformation Officer, players learn how actors deploy trolling, artificial amplification on social media, emotional language, and escalation to violence to spread disinformation.

According to research by the University of Cambridge Social Decision-Making Lab, published in the Harvard Misinformation Review, players are statistically significantly better at discerning between reliable and unreliable information and are much less likely to share bad information on social media, after playing the game. Thanks to ongoing monitoring and evaluation of the game's more than 400 000 plays, GEC determined that in some cases, players were coming away sceptical of all information, not just unreliable information. GEC and the studio behind the game developed a new feature in the game that corrects this issue.

Cat Park launched in October 2022 and is currently available in six languages. Players take the role of a person recruited into a social media pressure campaign. Players "train" with a group of activists with different media manipulation skillsets – creating sensational headlines, memes, and synthetic media – to stop a hypothetical development of a cat park.

The game has been played more than 100 000 times and there is a lesson plan available for most of the game's languages. Drawing on lessons from Harmony Square and research from the U.S. Agency for International Development that questioned the efficacy of media and information literacy projects in developing countries, Cat Park offers a much greater level of localisation. When players in Sub-Saharan Africa play the game in Amharic or Swahili the plot and characters will look different. When players in the Middle East and North Africa play the game in Arabic, the plot and characters will look different. Similarly, when someone plays the game in Spanish in Latin America, the game will look different. Research from the University of Cambridge published in Nature found that after playing the game, players are more sceptical of unreliable information.

Note: Harmony Square game link: https://harmonysquare.game/; Cat Park game link: https://catpark.game/
Source: Roozenbeek and van der Linden (2020[42]) "Breaking Harmony Square: A game that "inoculates" against political misinformation", *Harvard Kennedy School Misinformation Review*, https://doi.org/10.37016/mr-2020-47; Neylan, J. et al. (2023[43]), "How to "inoculate" against multimodal misinformation: A conceptual replication of Roozenbeek and van der Linden (2020)", *Scientific Reports*, Vol. 13/1, https://doi.org/10.1038/s41598-023-43885-2.

A focus moving forward will be on developing methods for measuring impact of these initiatives as they relate to the public's ability to take part constructively in the information space. This will require monitoring changes in broad indicators over time, such as susceptibility to mis- and disinformation narratives and trust in governmental communications and institutions. While direct causality is difficult (or impossible) to identify, these could be seen as possible pieces of evidence of success. Such analysis would be particularly relevant for large-scale projects that include considerable part of countries' population. Indeed, greater emphasis on longitudinal impact evaluations would enable comparisons against baselines, highlighting changes over time in the capacity for individuals to critically and reflectively consume information.

Analysis could also be based on the monitoring of specific behaviour of the audiences targeted by a policy or project. For example, this could include analysis of online activity such as changes in patterns of sharing mis- and disinformation materials following MIL trainings. There are clear limitations for such activities, however, including the lack of transparency of social media platforms. Finally, measurement could include self-assessments of the target audience following interventions or activities, for example via questionnaires given to participants who took part in an MIL initiative.

3.3. PUBLIC COMMUNICATION PLAYS AN IMPORTANT ROLE IN PROVIDING INFORMATION

A more immediate goal of whole-of-society efforts to strengthen societal resilience focuses on ensuring individuals are informed and aware of false and misleading content. In democratic settings where government information is open to scrutiny by free and independent media, the public communication function can play a crucial role in fostering societal resilience to disinformation. This is achieved by serving as a source of timely and relevant information. This function should aim to be distinct from political communication, which is linked to elections or political parties, political debates or the promotion of the government of the day. A modern public communication function should be understood as the government function to deliver information, listen, and respond to citizens in the service of the common good (OECD, 2021[44]). To that end, government efforts to build awareness and help ensure the public has access to information include the following avenues:

- In democratic environments where government information can be challenged by free and independent press, timely information provided by governments can build awareness of relevant challenges and threats
- Engagement with external partners, with appropriate governance models and within free and democratic contexts, can help build societal resilience to the spread of disinformation.

3.3.1. Accurate and timely information provided by public communication can build societal awareness of the risks of mis and disinformation

Information does not spread in a vacuum – traditional media and fact-checkers, online platforms, civil society, and individuals themselves are essential actors in generating and amplifying content. At the same time, governments, often via the public communication function of the centre of government or particular ministries, with other actors that constantly play a healthy checks and balance function, can help raise awareness of the spread of false and misleading content and serve as a source of accurate information. Even where facts are unclear or still being collected, as is often the case in crises, the public will demand updates; governments should consider how to anticipate and respond to individuals' needs honestly, transparently, and with the best information possible, while pre-empting the spread of rumours and falsehoods (OECD, 2023[28]). The public communication function therefore requires advanced and sophisticated governance to safeguard its focus on delivering for the public good, promote disclosure of sources, ensure a level of separation from political communications, as well as to build its capacity and professionalism. The OECD has conducted a comparative analysis of good practices and drawn from these a set of Good Practice Principles for Public Communication Responses to Mis- and Disinformation (Box 3.11). In most OECD countries, this function remains undervalued and underutilised as a source of information, and is still transitioning away from a focus on political communication.

Box 3.11. OECD Good Practice Principles for Public Communication Responses to Mis- and Disinformation

The OECD has developed 9 Principles of Good Practice to provide policymakers with guidance to address the spread of mis- and disinformation, and in turn strengthen information ecosystems and support democracy. They relate most directly to public communication interventions. The Principles are based on the analysis and review of relevant emerging practices in the field of countering mis- and disinformation and the factors that make them effective. The 9 principles are:

Structure and governance

1. **Institutionalisation**: Governments should consolidate interventions into coherent approaches guided by official communication and data policies, standards and guidelines. Public communication offices will benefit from adequate human and financial resources, a well-co-ordinated cross-government approach at national and sub-national levels, and dedicated and professional staff.
2. **Public-interest-driven**: Public communication should strive to be independent from politicisation in implementing interventions to counteract mis- and disinformation. Public communication should be separate and distinct from partisan and electoral communication, with the introduction of measures to ensure clear authorship, impartiality, accountability, and objectivity.
3. **Future-proofing and professionalisation:** Public institutions should invest in innovative research and use strategic foresight to anticipate the evolution of technology and information ecosystems and prepare for likely threats. Counter misinformation interventions should be designed to be open, adaptable and matched with efforts to professionalise the function and build civil servants' capacity to respond to evolving challenges.

Providing accurate and useful information

4. **Transparency**: Governments should strive to communicate in an honest and clear manner, with institutions comprehensively disclosing information, decisions, processes and data within the limitations of relevant legislation and regulations. Transparency, including about assumptions and uncertainty, can reduce the scope for rumours and falsehoods to take root, as well as enable public scrutiny of official information and open government data.
5. **Timeliness**: Public institutions should develop mechanisms to act in a timely manner by identifying and responding to emerging narratives, recognising the speed at which false information can travel. Communicators can work to build preparedness and rapid responses by establishing co-ordination and approval mechanisms to intervene quickly with accurate, relevant and compelling content.
6. **Prevention**: Government interventions should be designed to pre-empt rumours, falsehoods, and conspiracies to stop mis- and disinformation narratives from gaining traction. A focus on prevention requires governments to identify, monitor and track problematic content and its sources; recognise and proactively fill information and data gaps to reduce susceptibility to speculation and rumours; understand and anticipate common disinformation tactics, vulnerabilities and risks; and identify appropriate actions, such as "pre-bunking".

Democratic engagement, stronger media and information ecosystem

7. **Evidence-based**: Government interventions should be designed and informed by trustworthy and reliable data, testing, and audience and behavioural insights. Research, analysis and new insights can be continuously gathered and should feed into improved approaches and practices. Governments should

focus on recognising emerging narratives, behaviours, and characteristics to understand the context in which they are communicating and responding.

8. **Inclusiveness**: Interventions should be designed and diversified to reach all groups in society. Official information should strive to be relevant and easily understood, with messages tailored for diverse publics. Channels, messages, and messengers should be appropriate for intended audiences, and communication initiatives conducted with respect for cultural and linguistic differences and with attention paid to reaching disengaged, underrepresented or marginalised groups. Adequate resources and dedicated efforts can support responsive communication and facilitate two-way dialogue that counteracts false and misleading content.
9. **Whole-of-Society**: Government efforts to counteract information disorders should be integrated within a whole-of-society approach, in collaboration with relevant stakeholders, including the media, private sector, civil society, academia and individuals. Governments should promote the public's resilience to mis- and disinformation, as well as an environment conducive to accessing, sharing and facilitating constructive engagement around information and data. Where relevant, public institutions should co-ordinate and engage with non-governmental partners with the aim of building trust across society and in all parts of the country.

Source: OECD (2023[28]) "Good practice principles for public communication responses to mis- and disinformation", *OECD Public Governance Policy Papers*, No. 30, OECD Publishing, Paris, https://doi.org/10.1787/6d141b44-en.

Similarly, the European Centre of Excellence for Countering Hybrid Threats stressed the importance of rapidly refuting lies and debunking disinformation, the necessity of working with civil society, ensuring that the relevant teams within governments are in place, undermining foreign malign actors through humour and accessible messages, and learning from and supporting partners as best practices in countering disinformation threats. Many of the lessons drawn from government and civil society responses in Ukraine to Russian disinformation can provide important lessons for effective strategic communication efforts moving forward (Kalenský and Osadchuk, 2024[45]).

Building capacity, establishing clear frameworks and institutional mechanisms, and formalising definitions, policies and approaches can help shift from ad-hoc and fragmented public communication approaches to counteracting mis- and disinformation, to more structured and strategic approaches (OECD, 2021[44]). Along those lines, for example, the UK Government Communication Service Propriety Guidance specifies that government communication should be: relevant to government responsibilities; objective and explanatory; not represented as party political; conducted in an economic and appropriate way; and able to justify the costs as an expenditure of public funds (Government of the UK, 2022[46]).

Public communication campaigns and government websites can debunk existing disinformation narratives. Delivering clear and tailored messages can help ensure communications reach all segments of society, including groups that are less likely to be exposed to or trust official sources. To that end, preparing and implementing strategic communication campaigns and ensuring accurate content reaches target audiences are essential in counteracting the spread of mis- and disinformation (OECD, 2023[28]). For instance, in New Zealand, the "Unstoppable Summer" campaign, including television advertisements and a short musical video featuring the Director General of Health, and shown before broad audience events, is a good example of an effort to reach youth (Government of New Zealand, 2020[47]) (OECD, 2023[48]). Indeed, throughout the COVID-19 response, many countries developed processes that utilised credible messengers, such as members of a particular community, scientists and doctors, or influencers to present relevant information in a timely, authoritative, and non-politicised way to help ensure it reached as wide a segment of the population as possible.

Given their sensitive role in creating and sharing content, as well as monitoring and responding to disinformation, governments should take extra precautions to ensure their communication activities do not lead to allegations or instances of politicisation and

abuse of power. In the first instance, therefore, ensuring public communication strengthens information integrity depends on free information spaces and a strong and free media environment.

A lack of transparency around the activities of the public communication function can also undermine trust. Specifically, there is a risk that public communication initiatives designed to respond to disinformation can play into the arguments of actors who may accuse the government as playing "arbiter of truth" or even adopting disinformation techniques themselves. As a reaction to changing information consumption patterns, for example, governments have collaborated with online influencers to conduct awareness raising and other campaigns to reach segments of the population that they may not otherwise be well-suited to reach. While government engagement influencers via both paid and earned support can help strengthen the inclusiveness and reach of messages, putting in place clear guidelines, transparent processes, and independent oversight of the public communication function will help provide the necessary governance mechanisms to build trust (OECD, forthcoming[49]). More broadly, promoting access to information and open government standards, including publicly accessible open data, can help lower barriers for journalists and citizens to access public information and officials.

3.3.2. Engagement with non-government actors should be transparent and guided by clear and democratic oversight

Beyond the public communication function, how governments engage with online platforms, civil society, media, and academics needs to be carefully considered. On the one hand, facilitating open lines of communication between actors can be a fast and efficient way to identify threats and promote better functioning information spaces (see Box 3.12). It can also be important for government institutions to receive direct updates from online platforms about the spread of mis- and disinformation, such as concerted amplification operations by hostile actors or those that threaten elections and the safety of the public. Furthermore, much of the work to counteract disinformation threats remains sensitive due to national security considerations; providing too much insight into what is known about foreign information threats or efforts to counteract them also risks compromising their efficacy (OECD, forthcoming[49]).

Box 3.12. Lithuanian government co-operation with Debunk.EU and Meta on moderation policies

In 2022, the Government Chancellery of Lithuania initiated discussions with Meta on its content moderation policies related to the Russian aggression against Ukraine and activity on Facebook that appeared to filter content and block authors expressing support for Ukraine. The Lithuanian government, working with the Lithuanian CSO Debunk.eu, collected examples of accounts that had been blocked or deleted because they had expressed pro-Ukraine opinions, though had not otherwise violated Meta's content policies.

An outcome of the meeting was that it provided critical cultural and linguistic context to better inform Meta's content moderation policy and to ensure it considered the cultural and linguistic traditions of Lithuania. Indeed, Meta was often blocking accounts for words and expressions that it treated as offensive, despite their common and well-established use in the Lithuanian language. The engagement also facilitated consultation with Lithuanian language institutions, leading Meta to update its target keyword list and moderation policies.

The government and CSOs alike also noted that redress mechanisms were insufficient, and that blocking the posts and accounts of influential opinion makers without the possibility of correcting the content unreasonably limits free expression, restricts public debate, and can hinder civic initiatives, such as collection campaigns for victims in Ukraine. Meta representatives offered to hold training sessions with user groups to provide additional details of content management policies to help ensure their posts would not be blocked, as well as highlight the issues with senior management.

In 2023, 63% of Lithuanian citizens named social media as the primary place where they encounter disinformation, while the same percentage indicated that social media platforms' actions to minimise spread of disinformation was insufficient.

Source: Data provided by the Lithuanian government.

On the other hand, government interactions with online platforms, media, and other non-governmental actors in fighting mis- and disinformation are particularly sensitive given the risk that engagement with these external partners may enable governments to encourage content moderation beyond the formal regulatory power they have and infringe on freedom of expression.

Similar considerations point to the challenges of working with external partners to identify and debunk specific pieces of content. Notably, fact-checkers can be accused of political bias, and there is a risk that if fact-checkers receive direct funding or other support from governments, they will be pressured or incentivised (or perceived as being pressured or incentivised) to protect the government or smear political opponents. Research has found correlations between fact-checkers' political affiliations and their priorities and findings (Louis-Sidois, 2022[50]). The risk of perceived (or actual) politicisation by fact-checkers can also be seen by findings from the United States that demonstrated that Americans are split in their views of fact-checkers: Half said fact-checking efforts by news outlets and other organisations tend to deal fairly with all sides, while about the same portion (48%) say they tend to favour one side (Pew Research, 2019[51]).

In 2023, Faktograf, a Croatian fact-checking outlet, published the preliminary results from a survey of 41 leading European fact-checking organisations that illustrates the potency of the polarised environment in which they are working. Their research found that 90% of the outlets reported having experienced some type of harassment. More than three-quarters – 36 out of 41 – of the fact-checking organisations surveyed have experienced harassment online, often facing verbal attacks. Furthermore, 70% of the respondents that experienced online harassment were subjected to campaigns that include prolonged or co-ordinated threatening behaviour, such as stalking, smear campaigns, "doxing", and technology-facilitated gender-based violence, including gendered disinformation. Furthermore, 78% of the organisations confirmed that elected officials had targeted them directly (Faktograf, 2023[52]). In politically polarised environments, government engagement with these actors may risk amplifying risks and fuelling accusations of censorship and partisanship, harming both government and non-government actors in the process.

Self-regulation mechanisms put in place by media, CSOs, and other non-governmental actors involved in fact-checking and other relevant activities can help mitigate these challenges. In this regard, the active participation of media professionals can help ensure that journalistic expertise and ethical standards inform other relevant actions to promote information integrity. For instance, the International Fact-Checking Network (IFCN) has developed a code of principles signed by more than 200 fact checking organisations from around the world (IFCN, 2023[53]). Notably, IFCN signatory status may not be granted to organisations whose editorial work is controlled by the state, a political party or politician. It may, however, be granted to organisations that receive funding from state or political sources if the IFCN assessor determines there is clear and unambiguous separation of editorial control from state or political influence. Signatories also promise to be neutral and unbiased and commit to funding and organisational transparency. More detailed commitments are included in the "European Code of Standards for Independent Fact-Checking Organisations", approved by the European Fact-Checking Standards Network Project (supported by the European Commission) in August 2022. The emphasis in this Code is devoted to political impartiality and transparency of organisations' activities (EFCSN, 2022[54]).

Opportunities also exist for governments to be more transparent in their work with online platforms. For example, while decisions to take down content or add warning labels rest with the platforms themselves, governments may flag false or misleading content to platforms. In these cases, transparency around such discussions is critical and relevant disclosure mechanisms should be put in place (Full Fact, 2022[55]).

Transparency around how and under what circumstances governments share information with online platforms can be an important way to strengthen public confidence that freedom of expression is upheld, while at the same time enable external scrutiny that such actions are necessary. In addition, governments could consider establishing independent oversight mechanisms to evaluate their actions in this space and ensure they do not limit freedom of expression (OECD, forthcoming[49]).

3.4. STRENGTHENING PUBLIC PARTICIPATION AND BUILDING UNDERSTANDING OF THE INFORMATION SPACE THROUGH RESEARCH ARE KEY TO INFORMING POLICYMAKING AND IMPLEMENTATION

Building information integrity requires greater understanding of the specific problems that policy responses look to solve. As governments seek to strengthen their ability to counter threats posed by malign interference and disinformation, as well as reinforce the public's ability to participate in well informed democratic debate more widely, they will need to build the understanding of what conditions within the information environment foster democracy and encourage active citizen participation (Wanless and Shapiro, 2022[4]). Working with the public and non-governmental partners to develop this understanding, build trust, and inform effective policymaking can ultimately serve as a catalyst for good governance and democracy.

Strengthening participation and engagement suggests the following entry points on which to build:

- Participatory and deliberative democracy mechanisms can help establish policy priorities to strengthen information integrity.
- Government-funded research on information integrity should be conducted with clear objectives and guardrails and inform the policymaking and implementation process.

3.4.1. Participatory and deliberative democracy mechanisms can help deliver policies on strengthening information integrity

Governments can also develop participation initiatives to facilitate engagement with the public, media professionals, platforms, academics and civil society organisations more widely on strengthening information integrity and countering mis- and disinformation. If structured well, such initiatives can help raise awareness and set a policy agenda that reflects public priorities while also building trust between individuals, media and decision makers. In a field such as information integrity, in which public scrutiny about government interference in the information space is, rightfully, important, and at a time of low trust in public institutions (OECD, 2022[56]), promoting civic education and involving citizens and various stakeholders in the design of these policies will be important.

Opportunities for citizens' and stakeholders' participation and engagement are rooted in open and democratic governance and have multiplied significantly across OECD countries and beyond in the last decade. Indeed, the OECD Recommendation on Open Government notes that citizens should be provided "equal and fair opportunities to be informed and consulted and actively engaged in all phases of the policy-cycle," and that "specific efforts should be dedicated to reaching out to the most relevant, vulnerable, underrepresented, or marginalised groups in society, while avoiding undue influence and policy capture (OECD, 2017[57])." In this sense, the role of citizens refers to the public broadly, rather than the more restrictive sense of a legally recognised national of a state. Promoting the role of citizens and civil society means governments must create the conditions for the equitable, sustained, and substantive participation of civil society in policymaking (Forum on Information and Democracy, 2023[58]), and that countries should provide a level playing field by granting all stakeholders fair and equitable access to the development and implementation of public policies (OECD, 2010[59]).

Representative democracy, where citizen preferences are expressed through elected representatives, and direct democracy, where citizens vote on specific issues, are the most common avenues for participation. Beyond representation, promoting citizen participation should incorporate methods that provide the public with the

time, information, and resources to discuss and deliberate, produce quality inputs, and develop individual or collective recommendations to support more open policy-making. For example, online calls for submissions, public consultations and roundtable discussions are all examples of participatory mechanisms. Furthermore, putting in place effective deliberative democracy mechanisms that bring together a representative group of people to discuss issues and feed a "representative" view into decision-making processes can lead to better policy outcomes, enable policy makers to make hard choices, and enhance trust between citizens and government (OECD, 2020[60]).[3]

To-date, engagement initiatives on topics of information integrity have been relatively limited, likely reflecting the need to continue to build understanding around the trends, processes, and clarity of potential policy responses. Nevertheless, while often characterised as a technical matter, identifying policy initiatives related to strengthening information integrity are largely understandable by, and of interest to, the public. Beyond academics and other stakeholders, such as media, CSOs, and the private sector, public consultations can help inform and support efforts to build information integrity.

In 2020, Ireland established the Future of Media Commission as an independent body to undertake a comprehensive and far-reaching examination of Ireland's broadcast, print and online media. Notably, one of the recommendations of the report that was prepared by the Commission was for the government to create a National Counter-Disinformation Strategy (see Box 3.13), illustrating how public engagement can direct government actions and interventions. A similar example can be found in France with the organisation of the General Assembly on Information (*les États généraux de l'information"),* launched at the initiative of the President of the Republic in July 2023 with the aim of establishing a diagnosis of the key challenges related to the information space and proposing concrete actions that can be deployed at national, European, and international levels. The final output of this process, taking place between fall 2023 and summer 2024, will be to develop a set of proposals to anticipate future developments in the information space. Five working groups will develop these proposals, which will integrate feedback through citizens' assemblies and debates organised in-person in France as well as via an online consultation carried out by the French Economic, Social and Environmental Council (EESC).

Box 3.13. Ireland's Future of Media Commission

Established by the Irish government in September 2020, the Future of Media Commission is an independent body that explored, among other topics, how Ireland's media can remain sustainable and resilient in delivering on public service aims until 2030, including ensuring access to high-quality and impartial journalism.

Published in July 2022, the Future of Media Commission Report reflects the commission's core mission to develop recommendations on sustainable public funding of Irish media and to ensure its viability, independence, and capacity. The Commission's consultative efforts engaged the public, media organisations and industry stakeholders, regulators, and policymakers, and helped facilitate wide-ranging involvement in the drafting process.

The Commission's public consultation process received more than 800 written submissions, while its series of six online Thematic Dialogues saw more than 1 000 members of the public and 50 expert panellists engage in detailed discussions and debate. In addition, the Commission undertook a comprehensive survey to examine what the public consumes and values in terms of media content and what can be anticipated about future trends.

The report contains 50 recommendations, 49 of which were adopted in principle by the government upon publication, showing the value and relevance of the process and outputs. Notably, the report recommended creating a National Counter-Disinformation Strategy to tackle mis- and disinformation and improve general trust in information and media. The report also notes that the wider context of changing funding models in Ireland threaten to centralise information distribution, making the media landscape less plural, as advertising revenues move from media organisations to technology companies.

Source: Government of Ireland (2022[61]), Report of the Future of Media Commission, https://www.gov.ie/pdf/?file=https://assets.gov.ie/229731/2f2be30d-d987-40cd-9cfe-aaa885104bc1.pdf#page=null.

In 2022, Spain created the "Forum against Disinformation Campaigns in the Field of National Security", a platform for public-private collaboration to promote debate and reflection on the risks posed by disinformation campaigns in the field of national security.

The complexity of policymaking around building information integrity and the need to respond to the challenges faced also point to the value of deliberative democracy initiatives as a promising tool. These refer to the "direct involvement of citizens in political decision making, beyond choosing representatives through elections". Indeed, when conducted effectively, deliberative processes can lead to better policy outcomes, enable policymakers to make hard choices, and enhance trust between citizens and government (OECD, 2020[60]).

For example, the Canadian government worked with civil society organisations to organise three citizen assemblies on Democratic Expression, involving 90 Canadians who together contributed 6 000 volunteer hours to explore how the government should strengthen the information environment in which Canadians can freely express themselves. The Canadian Commission on Democratic Expression, in its report informed by the assemblies, recommended that the government should establish and independent Digital Services Regulator to set standards for the safe operation of digital services and to require platforms to conduct regular risk assessments. The Commission also recommended that the government appoint a special envoy to liaise at an international level on issues related to disinformation and foster dialogue with social media platforms, foreign governments, and multilateral bodies; promote interdisciplinary research on how content spreads; and to support media literacy efforts and invest in quality journalism at the national, regional and community levels (Citizens' Assembly on Democratic Expression, 2022[62]). In addition to their use in informing policymaking, deliberative processes also help counteract polarisation and disinformation, as research suggests that deliberation can be an effective way to overcome ethnic, religious, or ideological divisions between groups (OECD, 2020[60]).

3.4.2. Government-funded research on information integrity should be conducted with clear objectives and guardrails and inform the policymaking and implementation process

The aim of research in this space should be to better understand the conditions within the information environment that can foster healthy democratic societies and encourage active citizen participation (Wanless and Shapiro, 2022[4]). OECD members have responded to information threats in part by funding research activities to analyse trends, including the susceptibility to mis- and disinformation by different sectors of the population, content consumption patterns, and the threats posed by foreign actors producing and intentionally spreading false and misleading information. Governments are also supporting research to develop methodologies to assess the efficiency of various policy measures such as awareness campaigns and regulatory interventions. For example, Luxembourg financially supports the University of Luxembourg in its activities regarding the conduct of surveys for the European Media Pluralism Monitor and the "Local Media Project for Democracy", in full accordance with the principles of academic freedom and scientific independence.

Internal research conducted by or for the government can play an important role in supporting a better-informed policymaking process, particularly if it involves access to sensitive, private, or classified data. For example, the Government of Canada, in partnership with the OECD and the French Government, conducted an experiment to investigate Canadians' intentions to share different types of content on social media to better understand vulnerable populations and to design innovative policy solutions to mitigate the spread of misinformation (see Box 3.14).

Box 3.14. An International Collaboration to tackle Misinformation with Behavioural Insights

In partnership with the OECD and the French government, the Government of Canada implemented a Randomised Controlled Trial (RCT) embedded within the longitudinal COVID-19 Snapshot Monitoring Study (COSMO Canada) to test ways to reduce the spread of misinformation online. The study tested the effect of two behaviourally informed policy interventions. Both interventions were drawn from a rapidly growing research literature, and both aimed at improving the quality of news shared online (that is, the preference for sharing verifiably true over verifiably false news links) while prioritising individuals' autonomy. The first intervention was a simple accuracy evaluation prompt, attuning respondents' attention to accuracy by asking them to rate the accuracy of a single random headline prior to engaging with Facebook-style headlines online. The second intervention was a list of media literacy tips. This international collaboration found:

- First, data indicate a disconnect between participants' (N = 1872 participants) beliefs and sharing behaviours. People rate verifiably true headlines as significantly more accurate than verifiably false headlines (as determined by third-party fact-checkers), but are much less discerning in their sharing intentions – in other words, people share news headlines they believe to be false or questionable.
- Second, experimental results show that prompting participants with digital media literacy tips reduces their intention to share fake news online by more than 20%. While exposure to both the simple attention-to-accuracy prompt and the digital media literacy tips significantly increased participants' intentions to share true over false headlines, the effectiveness of the media literacy intervention far exceeded the effectiveness of the accuracy prompt. The digital media literacy tips had the greatest impact on reducing intentions to share false headlines online, reducing intentions to share by 21% compared to the control group (see figure below).

The findings from this RCT indicate that behavioural interventions can significantly reduce intentions to share false news headlines in online settings. The key insights from this report are the following:

1. A comprehensive policy response to mis- and disinformation should thus include an expanded understanding of human behaviour.

2. By empowering users, behavioural science offers effective and scalable policy tools that can complement system level policy to better respond to misinformation.
3. International experimentation across governments is vital for tackling global policy challenges and generating sustainable responses to the spread of mis- and disinformation.

These results provide compelling support for how simple and scalable online interventions presented to individuals before they engage with news stories may improve the quality of information circulating online. For some, it may be surprising to hear that individuals are (sometimes) willing to share news that they believe to be false or questionable. This study provides evidence that this does indeed happen, likely due to a failure to pay attention to the accuracy of news content confronted in the social media context. Although additional research and analysis is required to determine why individuals may choose to share false or misleading headlines online, studies like these remain vital for challenging assumptions about human behaviour, creating more effective and scalable solutions based on those they aim to serve, and indicating areas of future exploration that can enhance the robustness of knowledge on global behavioural challenges like mis- and disinformation.

Source: OECD (2022[63]), "Misinformation and disinformation: An international effort using behavioural science to tackle the spread of misinformation", *OECD Public Governance Policy Papers*, No. 21, OECD Publishing, Paris, https://doi.org/10.1787/b7709d4f-en.

Though governments may not disseminate the results of such research publicly, they can serve an important role in building understanding of the information space. Co-operation with external researchers to provide public outputs, on the other hand, allows governments to receive diverse insights and advice. Continuing to develop partnerships that are transparent, well-resourced, and that serve clear objectives will be important moving forward.

For example, Canada's Digital Citizen Initiative focuses on helping Canadians understand online disinformation and its impact on Canadian society, and building the evidence base to identify possible actions and future policymaking in this space (see Box 3.15 and (Government of Canada, 2023[64]). In the Netherlands, the Ministry of the Interior and Kingdom Relations is one of the partners collaborating in the AI, Media and Democracy Lab, an alliance between the University of Amsterdam, the Amsterdam University of Applied Sciences, and the Research Institute for Mathematics & Computer Science in the Netherlands to work with media companies and cultural institutions to increase knowledge related to the development and application of generative AI tools (in 2022, the project received EUR 2.1 million).

Box 3.15. Canada's Digital Citizen Initiative

Initiated by the Federal Government, Canada's Digital Citizen Initiative (DCI) funds civil society organisations, educational institutions, and research institutions to better understand and strengthen resilience against online disinformation and other online harms.

Since its inception in 2020, the DCI's Digital Citizen Contribution Program has provided over CAD 21 million in support of 110 projects. These projects include developing awareness and learning materials for the public, students, and educators, and supporting research to investigate the creation and spread of disinformation across Canada.

Ten separate calls for proposals have prioritised specific issues related to online disinformation and online harms. In the immediate wake of the COVID-19 pandemic, two calls for proposals provided CAD 3.5 million to amplify the efforts of organisations supporting individuals' abilities to identify and limit the spread of health-related mis- and disinformation. Following Russia's war of aggression against Ukraine, a targeted call in 2022 funded initiatives to help individuals identify online mis- and disinformation related to this issue.

In the November 2022 Fall Economic Statement, the Government of Canada announced an extended investment of CAD 31 million over four years. In 2024-25, the programme will provide financial assistance for proposals that:

- develop and publish tools to support digital media and civic literacy skills among people in Canada outside of educational institutions and/or among seniors in Canada;
- develop and publish tools to help people in Canada identify content created and spread by bots and/or artificial intelligence;
- develop and publish tools to prevent and address online violence against women, girls and 2SLGBTQI+ communities, and other forms of technology facilitated violence;
- create resources to support children and parents in Canada to address and prevent cyberbullying;
- build technical capacity and expertise among small and medium sized civil society organisations seeking to address mis- and disinformation, hate speech, and cyberbullying;
- develop and publish tools to build resilience to mis- ad disinformation stemming from foreign governments targeting people in Canada, including diaspora communities, and;
- conduct research, testing and evaluation of tools or interventions related to any of the above priorities.

Source: Government of Canada (2023[64]), "Digital Citizen Initiative, https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html.

European Union institutions also illustrate whole-of-society models for long-term funding for research projects related to fighting disinformation, notably during the funding cycle of the Horizon 2020 programme (European Comission, 2023[65]). Indeed, the fight against mis- and disinformation is one of the main priorities of current (2021-2027) funding round of "Horizon Europe" programme. For example, the EUR 7 million vera.ai project (2022-2025) connects 14 partner organisations, including the European Broadcasting Union, Deutsche Welle, as well as research institutes, universities, private companies, and the news agency AFP. Together, the consortium aims to help develop AI solutions that can help to unmask and neutralise advanced disinformation techniques (VERA.AI, 2023[66]).

Another important, though less direct, approach to supporting research is illustrated by the EU's funding to the European Digital Media Observatory (EDMO), which connects civil sector organisations and academics for joint efforts to strengthen information integrity. The second phase of the project has funded the creation of national and multinational digital media research hubs across Europe with EUR 11 million through the Connecting Europe Facility. There are currently 14 regional EDMO hubs that cover the 27 EU member states and Norway. One of the most important strands of EDMO work is research activities focused on project mapping, supporting, and co-ordinating research activities on disinformation at the European level, including the creation and regular update of a global repository of peer-reviewed scientific articles on disinformation. Similarly, Canada has made a USD 4 million (CAD 5.5 million) investment to create the Canadian Digital Media Research Network (CDMRN), bringing together a range of Canadian research institutions, to further strengthen Canadians' information resilience by researching how quality of information, including disinformation narratives, impacts Canadians' attitudes and behaviours and by supporting strategies for Canadians' digital literacy.

Moving forward, the role and impact of closed groups and messages shared on encrypted services such as WhatsApp will need to be better understood. These platforms provide users with valuable privacy and safety functions but can also be important channels to spread mis- and disinformation, while their private and encrypted nature make understanding content spread on these channels impossible to analyse (OECD, 2022[67]). Another challenge faced in supporting research in this space is that research tools, such as specialised software or application programming interfaces (API) used to facilitate content and data sharing between applications are often prohibitively expensive, particularly for smaller research groups with

limited budgets. Access to data from social media platforms is also increasingly difficult to get.

In response to these challenges, the European Union Digital Services Act (DSA) partially addresses the issue of data availability for the researchers (as discussed further in Chapter II). Specifically, Article 40 of the DSA stipulates that, "providers of very large online platforms or of very large online search engines shall, within a reasonable period, as specified in the request, provide access to data to vetted researchers who meet the (specified) requirements, for the sole purpose of conducting research that contributes to the detection, identification and understanding of systemic risks in the Union" (European Union, 2022[6]).

A fundamental issue regarding research in this space is that there is often a disconnect between the research being conducted and the ability for governments to use evidence collected in policymaking and implementation. Researchers and governments have identified a shortage of efficient information exchange and co-operation formats between relevant actors at both the national and international level. To that end, the French government has supported the International Observatory on Information and Democracy, which is modelled on the Intergovernmental Panel on Climate Change (IPCC) to aggregate and synthesise existing research to better understand the information and communication space (see Box 3.16).

Box 3.16. The International Observatory on Information and Democracy

Under the stewardship of Reporters Without Borders (RSF) and with the support of the French government, the Partnership on Information and Democracy was established in 2019. Today with 52 state signatories, this non-binding international governance process advances safeguards for the information and communication space to ensure the right to reliable information, the cornerstone of democratic discourse and critical to democratic institutions. The Forum on Information and Democracy is the civil society-led implementing entity of the Partnership working to advance policy change, enhanced civic voice and participation in agenda-setting and policy discourse and strengthening of the information ecosystem.

A core project of the Forum, the International Observatory on Information and Democracy was established to advance a common understanding of the structure of the information and communication space and its impact on democracy. By bringing together the research community, civil society, states, regulators, and representatives from private corporations, the Observatory is modelled on the IPCC, in this case regarding the information and communication space. In this way, the Observatory facilitates interaction between knowledge producers and policymakers.

Through this democratic lens, the Observatory aggregates and synthesises existing research and available data via regular reports, which provide civil society leaders, researchers, academics, and policymakers a periodic global assessment of the information and communication space and its impact on democracy. The Observatory's work will inform the international community's efforts to foster the adoption of effective and proportionate regulatory and non-regulatory measures for the protection of human rights – including the right to reliable information – and democracy in the digital space.

Reports of the Observatory explain existing state-of-the-art research. The aim is to help ensure stakeholders share a common understanding of critical impacts while also revealing research data gaps and important variance across different regions. The Observatory employs a robust methodology that ensures inclusion of perspectives and expertise from the Global Majority. With a governance structure led by international experts from the scientific community and civil society, yet conducting direct consultations with private and public officials, the Observatory contributes to creating shared knowledge benchmarks to help realign regulatory policy to ensure technology serves the public interest.

Observatory reports are addressed to governments, policymakers, regulatory bodies, NGOs, public information bodies, and technology corporations, to provide a shared understanding of how the current structure of the information and communication space is undermining democracies around the world. In turn, the Observatory's

ambition is to help stimulate meaningful dialogue, inform evidence-based policy decisions, and support innovative research in the field of the digital information space and democracy. The first work cycle will be completed in December 2024.

Source: Interview with Forum on Information and Democracy, February 2024.

Ultimately, for decision makers, it can be difficult to turn the results of academic studies into practical policies, suggesting that the feedback loop between researchers and governments can be improved to determine what conditions within the information environment are beneficial for democracy and help measure the success of policy interventions (Wanless and Shapiro, 2022[4]).

3.5. CONSIDERATIONS AND PATH FORWARD

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 healthy information and democratic spaces.

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.

REFERENCES

Basol, M. et al. (2021), "Towards psychological herd immunity: Cross-cultural evidence for two prebunking interventions against COVID-19 misinformation", *Big Data & Society*, Vol. 8/1, https://doi.org/10.1177/20539517211013868. [34]

Be media smart (2023), "Be media smart website", https://www.bemediasmart.ie/ (accessed on 15 February 2024). [22]

Citizens' Assembly on Democratic Expression (2022), , https://static1.squarespace.com/static/5f8ee1ed6216f64197dc541b/t/632c7bdbe8994a793e6256d8/1663859740695/CitizensAssemblyOnDemocraticExpression-PPF-SEP2022-FINAL-REPORT-EN-1.pdf. [62]

CLEMI (2023), *Bilan de formation 2021-2022*, https://www.clemi.fr/fr/bilans-de-formation.html. [35]

CLEMI (n.d.), *CLEMI website*, Centre pour l'éducation aux médias et à l'information, https://www.clemi.fr/fr/qui-sommes-nous.html (accessed on 15 February 2024). [18]

Council of Europe (2016), *Mapping of media literacy practices and actions in EU-28*, https://rm.coe.int/media-literacy-mapping-report-en-final-pdf/1680783500. [36]

EFCSN (2022), "The European Fact-Checking Standards Network Project", European Fact-Checking Standards Network, https://eufactcheckingproject.com/. [54]

European Comission (2023), "Funded projects in the fight against disinformation", https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation/funded-projects-fight-against-disinformation_en. [65]

European Commission (2023), *Guidelines pursuant to Article 33a(3) of the Audiovisual Media Services Directive on the scope of Member States' reports concerning measures for the promotion and development of media literacy skills*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023XC0223%2801%29. [12]

European Commission (n.d.), "DigComp", https://joint-research-centre.ec.europa.eu/digcomp_en. [41]

European Union (2022), *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*, Publications Office of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?ur. [6]

European Union (2018), *Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provis*, Publications Office of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1808. [7]

Faktograf (2023), *Harassment of Fact-checking Media Outlets in Europe*, https://faktograf.hr/site/wp-content/uploads/2023/03/preliminary-survey-report-final.pdf. [52]

Forum on Information and Democracy (2023), *OECD Tackling disinformation: Strengthening democracy through information integrity conference*. [58]

Forum on Information and Democracy (2023), *Pluralism of news and information in curation and indexing algorithms*, https://informationdemocracy.org/wp-content/uploads/2023/08/Report-on-Pluralism-Forum-on-ID.pdf. [14]

Full Fact (2022), *Full Fact Report 2022: Tackling online misinformation in an open society - what law and regulation should do*, https://fullfact.org/media/uploads/full-fact-report-2022.pdf. [55]

Government of Canada (2023), *Digital Citizen Initiative*, https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html. [64]

Government of Finland (2019), *Media Literacy in Finland: National Media Education Policy*, Ministry of Education and Culture, https://medialukutaitosuomessa.fi/mediaeducationpolicy.pdf. [16]

Government of Ireland (2022), *Report of the Future of Media Commission*, https://www.gov.ie/pdf/?file=https://assets.gov.ie/229731/2f2be30d-d987-40cd-9cfe-aaa885104bc1.pdf#page=null. [61]

Government of Netherlands (2022), *Government-wide strategy for effectively tackling disinformation*, https://www.government.nl/documents/parliamentary-documents/2022/12/23/government-wide-strategy-for-effectively-tackling-disinformation. [5]

Government of New Zealand (2020), *Make summer unstoppable by hitting COVID-19 for six*, https://www.beehive.govt.nz/release/make-summer-unstoppable-hitting-covid-19-six. [47]

Government of Portugal (2017), *Resolução do Conselho de Ministros n.º 142/2023*. [15]

Government of the UK (2022), *Government Communcation Service Propriety Guidance*, https://gcs.civilservice.gov.uk/publications/propriety-guidance/. [46]

Government of the UK (2022), "Help for vulnerable people to spot disinformation and boost online safety", https://www.gov.uk/government/news/help-for-vulnerable-people-to-spot-disinformation-and-boost-online-safety. [25]

Guess, A., J. Nagler and J. Tucker (2019), "Less than you think: Prevalence and predictors of fake news dissemination on Facebook", *Science Advances*, Vol. 5/1, https://doi.org/10.1126/sciadv.aau4586. [24]

Hill, J. (2022), "Policy responses to false and misleading digital content: A snapshot of children's media literacy", *OECD Education Working Papers*, No. 275, OECD Publishing, Paris, https://doi.org/10.1787/1104143e-en. [11]

IFCN (2023), "Commit to transparency — sign up for the International Fact-Checking Network's code of principles", International Fact-Checking Network, https://ifcncodeofprinciples.poynter.org/. [53]

Kalenský, J. and R. Osadchuk (2024), *How Ukraine fights Russian disinformation: Beehive vs mammoth*, https://www.hybridcoe.fi/wp-content/uploads/2024/01/20240124-Hybrid-CoE-Research-Report-11-How-UKR-fights-RUS-disinfo-WEB.pdf. [45]

Latvian State Security Service (n.d.), "Annual reports", https://vdd.gov.lv/en/useful/annual-reports (accessed on 15 February 2024). [30]

Louis-Sidois, C. (2022), "Checking the French Fact-checkers", *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.4030887. [50]

Maertens, R. et al. (2021), "Long-term effectiveness of inoculation against misinformation: Three longitudinal experiments", *Journal of Experimental Psychology: Applied*, Vol. 27/1, pp. 1-16, https://doi.org/10.1037/xap0000315. [33]

Media Literacy Ireland (n.d.), "What is Media Literacy Ireland?", https://www.medialiteracyireland.ie/ (accessed on 15 February 2024). [21]

Media literacy now (2022), *Media Literacy Policy Report 2022*, https://medialiteracynow.org/policyreport/. [13]

Media Literacy Week (2023), "Media Literacy Week celebrates diversity in creating and developing a better media environment for all", https://mediataitoviikko.fi/in-english/. [23]

Morris, K. (2023), *Ofcom's Toolkit for Evaluating Media Literacy Interventions*, Media & Learning Association, https://media-and-learning.eu/type/featured-articles/ofcoms-toolkit-for-evaluating-media-literacy-interventions/. [40]

Neylan, J. et al. (2023), "How to "inoculate" against multimodal misinformation: A conceptual replication of Roozenbeek and van der Linden (2020)", *Scientific Reports*, Vol. 13/1, https://doi.org/10.1038/s41598-023-43885-2. [43]

Norwegian Media Authority (2021), *Critical Media Understanding in the Norwegian Population*, https://www.medietilsynet.no/globalassets/publikasjoner/kritisk-medieforstaelse/211214-kmf_hovudrapport_med_engelsk_2021.pdf. [38]

Norwegian Media Authority (2021), *Stop, think, check: How to expose fake news and misinformation*, https://www.medietilsynet.no/english/stop-think-check-en/. [20]

OECD (2023), *Drivers of Trust in Public Institutions in New Zealand, Building Trust in Public Institutions,*, OECD Publishing, https://doi.org/10.1787/948accf8-en. [48]

OECD (2023), "Good practice principles for public communication responses to mis- and disinformation", *OECD Public Governance Policy Papers*, No. 30, OECD Publishing, Paris, https://doi.org/10.1787/6d141b44-en. [28]

OECD (2023), "What is resilience and how to operationalise it?", OECD, Paris, https://www.oecd.org/dac/conflict-fragility-resilience/risk-resilience. [1]

OECD (2022), *Building Trust and Reinforcing Democracy: Preparing the Ground for Government Action*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/76972a4a-en. [67]

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, https://doi.org/10.1787/b407f99c-en. [56]

OECD (2022), "Misinformation and disinformation: An international effort using behavioural science to tackle the spread of misinformation", *OECD Public Governance Policy Papers*, No. 21, OECD Publishing, Paris, https://doi.org/10.1787/b7709d4f-en. [63]

OECD (2022), *OECD Guidelines for Citizen Participation Processes*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/f765caf6-en. [68]

OECD (2022), *The Protection and Promotion of Civic Space: Strengthening Alignment with International Standards and Guidance*, OECD Publishing, Paris, https://doi.org/10.1787/d234e975-en. [3]

OECD (2022), *Trends Shaping Education 2022*, OECD Publishing, Paris, https://doi.org/10.1787/6ae8771a-en. [10]

OECD (2021), *21st-Century Readers: Developing Literacy Skills in a Digital World*, OECD Publishing, https://doi.org/10.1787/a83d84cb-en. [2]

OECD (2021), *OECD Report on Public Communication: The Global Context and the Way Forward*, OECD Publishing, Paris, https://doi.org/10.1787/22f8031c-en. [44]

OECD (2020), *Innovative Citizen Participation and New Democratic Institutions: Catching the Deliberative Wave*, OECD Publishing, Paris, https://doi.org/10.1787/339306da-en. [60]

OECD (2017), "Recommendation of the Council on Open Government", *OECD Legal Instruments*, OECD/LEGAL/0438, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0438. [57]

OECD (2010), *Recommendation of the Council on Principles for Transparency and Integrity in Lobbying*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0379. [59]

OECD (forthcoming), *Unlocking public communication's potential for stronger democracy and increased trust*. [49]

Ofcom (2023), *A toolkit for evaluating media literacy interventions*, https://www.ofcom.org.uk/research-and-data/media-literacy-research/approach/evaluate/toolkit. [39]

Ofcom (2023), *Making Sense of Media*, https://www.ofcom.org.uk/research-and-data/media-literacy-research. [8]

Pew Research (2019), *Republicans far more likely than Democrats to say fact-checkers tend to favor one side*, https://www.pewresearch.org/short-reads/2019/06/27/republicans-far-more-likely-than-democrats-to-say-fact-checkers-tend-to-favor-one-side/. [51]

Portuguese Regulatory Authority for the Media (2023), *Media Literacy in Portugal: 1st Report under No. 2 of Article 33.A of the Audiovisual Media Services Directive*, https://www.erc.pt/en/reports/media-literacy/1st-report-under-n-2-of-article-33-a-of-the-audiovisual-media-services-directive-eu-/. [17]

Republic of Lithuania (2022), *National Threat Assessment 2022*, State Security Department (VSD)/Defence Intelligence and Security Service under the Ministry of National Defence (AOTD), https://www.vsd.lt/wp-content/uploads/2022/04/ANGL-el-_.pdf. [31]

Roozenbeek, J. and S. van der Linden (2021), *Don't Just Debunk, Prebunk: Inoculate Yourself Against Digital Misinformation*, https://www.spsp.org/news-center/blog/roozenbeek-van-der-linden-resisting-digital-misinformation. [26]

Roozenbeek, J. and S. van der Linden (2020), "Breaking Harmony Square: A game that "inoculates" against political misinformation", *Harvard Kennedy School Misinformation Review*, https://doi.org/10.37016/mr-2020-47. [42]

Supo (2022), "Supo Yearbook 2021: Finns must be prepared for influencing efforts from Russia during NATO debate", SUPO Finnish Security and Intelligence Service, https://supo.fi/en/-/supo-yearbook-2021-finns-must-be-prepared-for-influencing-efforts-from-russia-during-nato-debate. [29]

Swedish Security Service (n.d.), "Sweden Security Police Yearbooks", https://www.sakerhetspolisen.se/om-sakerhetspolisen/publikationer/sakerhetspolisens-arsberattelse.htm (accessed on 15 February 2024). [32]

The Dutch Media Literacy Network (n.d.), "About Dutch Media Literacy Network", https://netwerkmediawijsheid.nl/over-ons/about-dutch-media-literacy-network/ (accessed on 15 February 2024). [19]

UK Department for Digital, Culture, Media & Sport (2021), *Online media literacy strategy*, https://www.gov.uk/government/publications/online-media-literacy-strategy. [37]

UNESCO (2023), *Media and information literacy*, United Nations Educational, Scientific and Cultural Organization, https://www.unesco.org/en/media-information-literacy#:~:text=Media%20and%20information%20literacy%20empowers,to%20information%2C%20and%20sustainable%20development. [9]

Van der Linden, S. (2023), *Foolproof: Why we fall for Misinformation and How to Build Immunity*, 4th Estate. [27]

VERA.AI (2023), *Project Summary: Facts & Figures*, https://www.veraai.eu/project-summary (accessed on 19 October 2023). [66]

Wanless, A. and J. Shapiro (2022), *A CERN Model for Studying the Information Environment*, https://carnegieendowment.org/2022/11/17/cern-model-for-studying-information-environment-pub-88408. [4]

NOTES

[1] For more information, see: https://www.mk.gov.lv/lv/media/14255/download

[2] For additional information, see: https://www.isdatechtzo.nl/

[3] For additional information, see OECD (2022[68]), *OECD Guidelines for Citizen Participation Processes*.

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

This chapter sheds light on how countries are upgrading their institutional architecture to strengthen information integrity. It analyses the role of strategic frameworks and effective intergovernmental co-ordination mechanisms within and between countries. Finally, it identifies the need to equip public officials with the skills and resources to better understand disinformation threats and to develop adapted regulatory governance that supports an enabling environment in which reliable information can thrive.

This chapter includes data from 24 OECD Member countries obtained from the survey "Institutional architecture and governance practices to strengthen information integrity" designed by the OECD DIS/MIS Resource Hub team (hereafter referred to as "the OECD survey"). Countries that responded to the survey include: Australia, Canada, Chile, Colombia, Costa Rica, Estonia, Finland, France, Germany, Greece, Italy, Ireland, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Portugal, Slovak Republic, Spain, Sweden, Switzerland, Türkiye and the United States.

4.1. INTRODUCTION

OECD governments are adapting their institutions and policy frameworks to respond to threats posed by disinformation and to create an enabling environment for accurate, reliable, and plural information to thrive. The challenge from a governance standpoint is significant, as governments find themselves in a complex position: policy measures are needed to counter disinformation and reinforce information integrity, and yet these actions should not result in greater control over publicly available information or undermine freedom of expression.

The range of threats that disinformation campaigns pose – from public health conspiracy theories to foreign information manipulation and interference operations, as recently seen in the context of the COVID-19 pandemic and Russia's manipulation of information to undermine international support for Ukraine (European Union External Action Service, 2023[1]) – have acted as a catalyst for governments to address this global phenomenon in a co-ordinated and comprehensive way.

Putting in place national strategic frameworks, administrative co-ordination units, task forces, and capacity building efforts – namely, institutional architecture – is essential as they respond to disinformation and implement measures that enhance information integrity. To that end, governments could asses their own institutional arrangements and practices, recognising that:

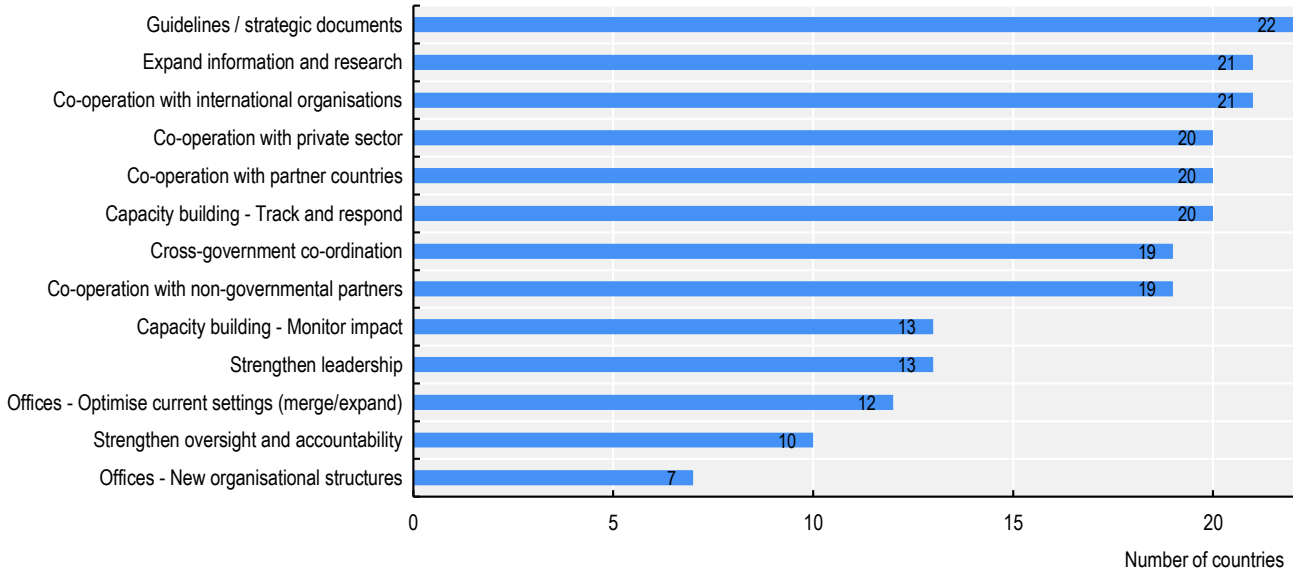
- Strategic guidance and co-ordinated policy efforts, both at the national and international level, are needed to effectively address the multifaceted and complex effort to build information integrity
- A constantly evolving information space requires governments to invest in capacity-building programmes and technology infrastructure within public administrations, enabling them to develop coherent and comprehensive policies to enhance information integrity
- Governments will need to adapt and upgrade regulatory governance that supports an enabling environment for reliable information to flourish.

4.2. GOVERNMENT CO-ORDINATION AND STRATEGIC GUIDANCE ARE NEEDED TO ADDRESS THIS MULTIFACETED POLICY CHALLENGE

A multifaceted challenge like disinformation, involving multiple actors, channels, and tactics, needs to be addressed in a co-ordinated and strategic manner. The scale and speed of the proliferation of false and misleading content has made countries aware of the need to develop a comprehensive view of how to improve the level of integrity in the information space. To this end, governments are increasingly setting up or upgrading their co-ordination mechanisms. Within countries, co-ordination mechanisms vary widely and can consist of central offices (units, cells…) or inter-agency task forces composed of public servants from across the government. The latter generally have focused mandates and scope.

The priority given to these aspects of governance response is clear: almost all respondents to the OECD survey identified developing, updating, or increasing the relevance of policy and/or strategy documents as a top priority[1] (Figure 4.1). Most respondent countries also flagged the importance of better co-ordination within and outside of government, as well as building their capacity to identify and respond to disinformation threats. These priorities provide a basis for understanding where governments can focus their efforts to develop more effective governance architecture in this policy area.

Figure 4.1. Areas for future improvements to strengthen information integrity



Note: n = 22
Source: OECD Survey on Institutional architecture and governance practices to strengthen information integrity, 2023.

4.2.1. Developing strategic frameworks to tackle disinformation and reinforce information integrity is a top priority

Strategic frameworks are essential to supporting a coherent vision and response to reinforcing information integrity. National strategies can provide clarity by establishing institutional responsibilities, preventing duplication of efforts, and helping avoid information asymmetries across government. That said, a strategy document is not an end in itself, but a means to guide the design of policy measures and evaluation timeframes to assess the efficiency and progress of the policies implemented (OECD, 2020[2]).

Some countries, particularly in recent years, have developed national strategies that specifically focus on tackling disinformation and reinforcing information integrity. However, data from the OECD survey shows that only nine countries (Australia, Estonia, Latvia, Lithuania, Portugal, Spain, Netherlands, Italy, and United States) have developed a strategic document providing direction on how to tackle disinformation and reinforce information integrity domestically.[2] Other countries, such as Ireland and Germany, are in the process of developing national strategies specifically focused on these issues.

Countries' strategies often cover operational aspects, such as the designation of focal points, the identification of functions of the co-ordination mechanism(s) and set time frames to ensure the efficient implementation and evaluation of progress (see Box 4.1 for an overview of the Netherlands' national strategy).

Box 4.1. The Netherlands' government-wide strategy for tackling disinformation

In December 2022, the Dutch Ministry of the Interior and Kingdom Relations, Ministry of Justice and Security, and Ministry of Education, Culture and Science presented to the House of Representatives a renewed government-wide strategy to protect the free and open public debate against disinformation.

In the document, they present their national strategy as an effective approach to tackling mis- and disinformation centred on the values and fundamental rights of the rule of law, such as the freedom of speech and press. An important point of the Netherlands' strategy is that they highlight that qualifying disinformation as such and conducting fact-checking are not primary duties for the government. The document does note, however, that where national security, public health, or social and/or economic stability are at stake, the government can act and debunk false and misleading information.

The strategy outlines that the Minister of the Interior and Kingdom Relations has a co-ordinating responsibility for the policy against disinformation and acts as the primary point of contact within the national government and toward municipal and provincial authorities. The ministry is to conduct this role by promoting collaboration between authorities in this area and by fulfilling a knowledge function. The strategy also emphasises the need for international co-ordination mechanisms, the European Rapid Alert System, the Hybrid Centre of Excellence and the NATO StratCom Centre of Excellence and international fora such as the European Union, G7, and the OECD. This strategy updates the first government-wide disinformation policy presented in 2019 (Parliamentary Documents II 2019/2020, 30821, no. 91).

Source: Government of the Netherlands (2022[3]), *Government-wide strategy for effectively tackling disinformation*, https://www.government.nl/documents/parliamentary-documents/2022/12/23/government-wide-strategy-for-effectively-tackling-disinformation.

Beyond national strategies, and particularly due to the multifaceted nature of this phenomenon, guidance on responding to disinformation and reinforcing information integrity is in many countries included as part of other national strategic documents. This is the case in Australia, Colombia, Costa Rica, Estonia, France, Finland, Germany, Luxembourg,[3] and Slovak Republic.

In Germany and Estonia, for example, measures addressing disinformation are outlined in their national security policy. The German National Security Strategy, adopted by the Federal Cabinet in June 2023, mentions diverse measures to prevent disinformation campaigns and to understand how they intersect with other national security threats. In Estonia, a course of action to tackle disinformation is stipulated in the National Security Concept (updated in February 2023). In Australia, policies to tackle disinformation are also part of their digital and foreign interference priorities, referenced in both Australia's International Cyber and Critical Tech Engagement Strategy and Australia's Counter Foreign Interference Strategy. In France, the National Strategic Review (*Revue nationale stratégique*, in French) presented by the French President in October 2022 provides an overview of the country's national and international defense and security environment, highlighting the fight against disinformation as a priority. The Review also led to the National Strategy on Influence, currently being drafted by the Ministry for Europe and Foreign Affairs, and to the creation of dedicated units to tackle disinformation within several ministries, including the Ministry for Europe and Foreign Affairs and the Ministry of Armed Forces.

Furthermore, the Slovak Republic adopted its Concept of Strategic Communication in June 2023, which looks to help the strategic communication function respond to and mitigate the harmful effects of influence operations in the information space and increase citizens' trust in democratic institutions. It outlines efforts to improve communication between the state and citizens, formalise and streamline co-operation and co-ordination of state institutions in strategic communication, and speed up the state's response in the fight against disinformation (Government of the Slovak Republic, 2023[4]).

Beyond the strategic framework itself, the process of developing, implementing, and subsequently monitoring a strategy demands attention. Indeed, an inclusive and rigorous strategy development process can help ensure that objectives promote democratic goals and are meaningful to citizens (OECD, 2020[2]). To ensure this, some countries have established working groups that help articulate this process. For instance, Ireland's National Counter Disinformation Strategy Working Group, created in 2023, resulted from a recommendation of Ireland's Future of Media Commission (FoMC) that called for a more co-ordinated and strategic approach to combat the damaging impact of disinformation on Irish society and democracy (Box 4.2).

Box 4.2. Ireland's National Counter Disinformation Strategy Working Group

In 2022, the Irish government created the "National Counter Disinformation Strategy Working Group" co-ordinated by the Department of Tourism, Culture, Arts, Gaeltacht, Sports, and Media. The body includes representatives from industry, academia, civil society and government departments.

As recommended by the Future of Media Commission, the working group is tasked with developing a National Counter Disinformation Strategy in consultation with all relevant departments and agencies, including Irish European Digital Media Observatory hub, industry stakeholders, news organisations, civil society groups, Irish fact-checkers and disinformation researchers. To this end, three sub-groups were set up to examine subject areas pertinent to disinformation, covering:

- The mapping of existing initiatives
- The examination of the current and emerging regulatory environment
- The support of free independent high-quality journalism and the protection of public interest information.

Each sub-group published a report on their subject area. The consultation period has now finished, and comprised a written public consultation and a consultation forum open to a wide range of stakeholders. It is intended that the Strategy will be published by the end of Q1 2024.

The Strategy aims to co-ordinate national efforts to combat disinformation and provide a joined-up approach to ensure effective restraints are applied to the creation and dissemination of this harmful material. The working group is also tasked with developing effective long-term monitoring of the application of the EU Code of Practice on Disinformation and the Digital Services Act in Ireland. Minutes of the meetings of the working group and other relevant documents are made public via the official government website.

Source: Government of Ireland (2023[5]), National Counter Disinformation Strategy Working Group, https://www.gov.ie/en/publication/04f9e-national-counter-disinformation-strategy-working-group.

As government efforts to build information integrity continue to develop, it will be worth advancing understanding on trends and priorities in order to clarify and strengthen the role of strategic guidance in this area.

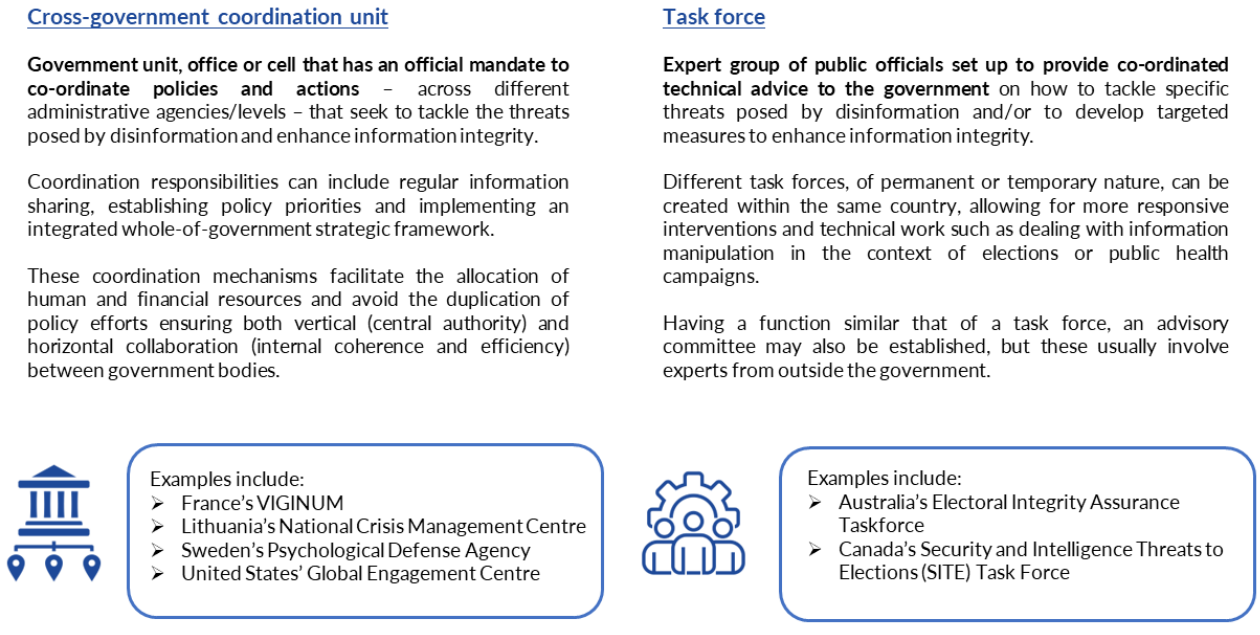
4.2.2. Government mechanisms to ensure co-ordinated policies in support of information integrity should have clear mandates and scope

A consistent multi-agency approach can help countries identify synergies between sectoral priorities, assign clear responsibilities, avoid duplication of efforts, and promote mutually supporting actions across institutions tackling disinformation. For example, establishing the operational capacity to track, pre-bunk, and debunk information manipulation campaigns often requires co-ordination at the strategic level, to put in place systems, processes, and monitoring functions, as well as at the tactical level to ensure actions can be taken in a timely manner.

The ways in which countries co-ordinate their responses to disinformation threats and efforts to enhance information integrity are varied and evolving rapidly. At the national level, responsibilities are found across the public sector, including the centre of government, line ministries (including security, digital, communication, media, culture, education, and research), security and intelligence agencies, and regulators. The complexity of efforts to reinforce information integrity in democracies calls for establishing co-ordination mechanisms to facilitate co-operation within and between governments.

Data from the OECD survey shows that half of respondent countries (54%) have at least one cross-government mechanism dedicated to co-ordinate national efforts to identify and respond to disinformation and/or to provide technical advice on policies related to this matter.[4] These are generally established either as central units (such as offices or cells) that have an official mandate to co-ordinate responsibilities, and/or as formal task forces or working groups composed of public servants from across the government (Figure 4.2).

Figure 4.2. Government co-ordination mechanisms to tackle disinformation

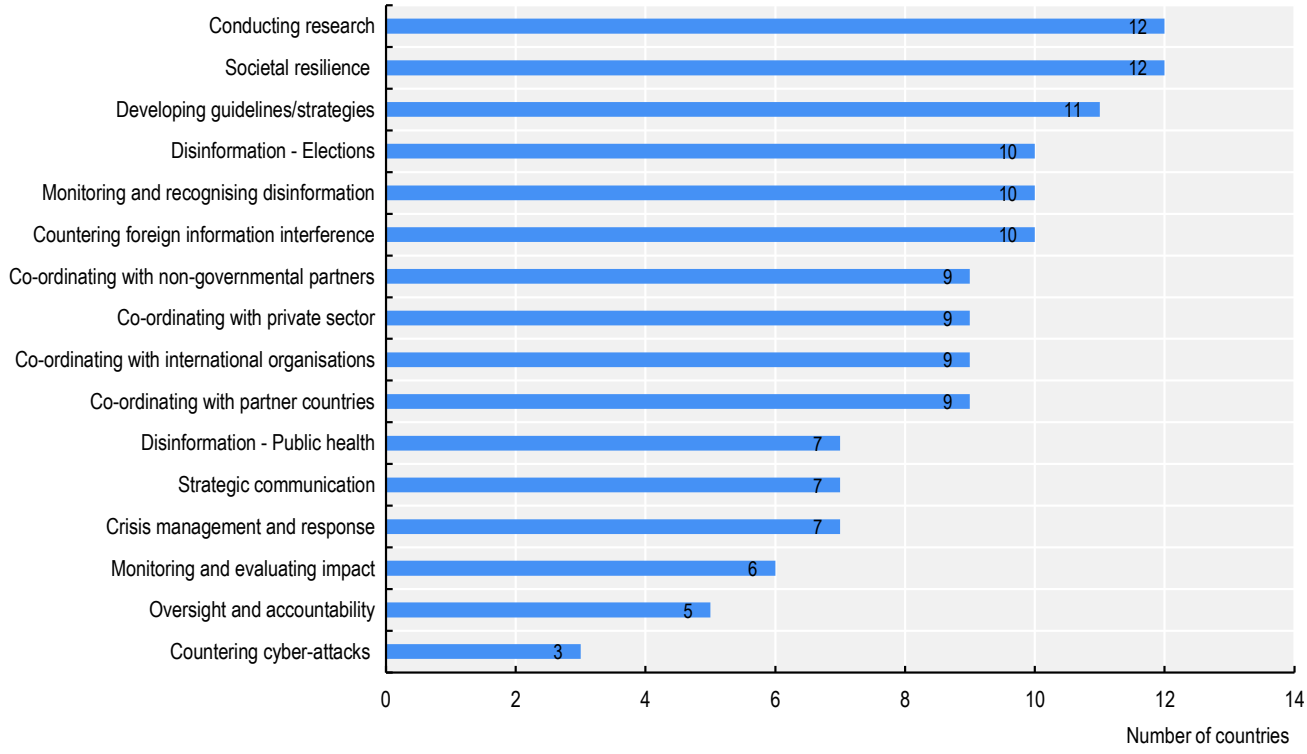


Source: Authors' elaboration.

Notably, the formation of co-ordination mechanisms has been a relatively recent effort, with all of them having been established, at least in their current form, since 2016. Given recent trends in disinformation, governments have struggled to define their roles in addressing such threats. The establishment of official offices or mechanisms has helped democratic governments understand and respond to these threats, including by providing clarity regarding the exact types of behaviour and content that government agencies should respond to (Kleis Nielsen, 2021[6]). Co-ordination groups also create focal points within governments that promote transparency, to help manage the risk that measures designed to combat disinformation exacerbate social distrust and mitigate unintended effects on freedom of expression and opinion (Butcher, 2019[7]).

Co-ordination mechanisms that have been established largely share priority objectives in relation to conducting research on disinformation dynamics, increasing societal resilience to the spread of false and misleading information, and developing or increasing relevance of guidelines and/or strategic documents (Figure 4.3).

Figure 4.3. Objectives cross-government co-ordination mechanism



Note: n = 13 countries.
Source: OECD Survey on Institutional architecture and governance practices to strengthen information integrity (2023).

Cross-government co-ordination units

Regarding cross-government co-ordination mechanisms, survey responses and available public information suggest that countries have generally developed legal frameworks that define the parameters within which these mechanisms can operate. These legal provisions are particularly important to explain the scope of action of the co-ordination mechanism, to establish internal controls and reporting procedures for its activities, and to reduce the risk of possible abuse of public policy measures.

Indeed, cross-government co-ordination mechanisms and units need to have clear mandates and be explicitly prevented from intervening in policy areas that could endanger freedom of expression and undermine democratic quality. To that end, in May 2023, Latvia approved the by-laws of the National Coordination Group on Information Space Security. These by-laws define the legally binding rules that the mechanism uses to operate and establishes the State Chancellery's Strategic Communication Coordination Department as the central managing authority (Box 4.3).

Box 4.3. The National Co-ordination Group on Information Space Security – Latvia

The National Information Space Security Co-ordination Group is a consultative body that facilitates co-operation and exchange of information between the institutions involved in responding to and mitigating relevant security risks and challenges.

Led by the State Chancellery's Strategic Communication Co-ordination Department (StratCom), this group has two main functions: (i) to co-ordinate and oversee the implementation of the Conceptual Report on the State Strategic Communication and Security of the Information Space for 2023-2027; and (ii) to facilitate the detection, reduction, and prevention of risks and threats to the State information space and public security.

The bodies that are part of such group include: the Chancery of the President, the Ministries of Culture, Foreign Affairs, Interior, Defence, Justice, Environmental Protection and Regional Development, Finance, Transport, Education and Science, Economy, the Prime Minister's Office, the State Security Service, the State Police, National Council for Electronic Media, the Council for Public Electronic Media, the Information Technologies Security Incidents Response Institution CERT.lv, and the Office for the Protection of the Constitution.

Source: Latvijas Vēstnesis (2023[8]), "Valsts informatīvās telpas drošības koordinācijas grupas nolikums", https://likumi.lv/ta/id/341811-valsts-informativas-telpas-drosibas-koordinacijas-grupas-nolikums.

One key function is the need for governments to respond rapidly and often within the news cycle, particularly during crises, to ensure accurate information is being shared and prevent false or misleading content from taking hold. Information crisis structures are an important tool in this regard. In Lithuania, the National Security Strategy established the creation of the National Crisis Management Centre (NKVC), a focal point and situation centre to co-ordinate responses to national security threats, including disinformation (Box 4.4).

Box 4.4. The National Crisis Management Centre – Lithuania

Since 2017, disinformation threats directed to Lithuania have been managed by the Chancellery of the Government as established by the country's National Security Strategy. In 2022, the National Crisis Management Centre (NCMC) was set up as the body to co-ordinate crisis prevention and management, including the state's response to disinformation at the national level. In the case of a crisis or emergency, the Centre proposes responses and solutions, supports their implementation, and facilitates inter-institutional co-ordination.

Within the NCMC, a Strategic Communication Coordination Task Force co-ordinates strategic communication in the field of national security via:

- A cross-government task force (consisting of weekly meetings and Signal chats)
- Co-operation with municipalities (via Signal chats).
- Engaging civil society and academic experts (via quarterly meetings and Signal chats)
- Engagement with media (via Signal chats)

This model was tested successfully during the 2023 NATO summit in Vilnius. To formalise and strengthen the model, in 2024, the NCMC will create a cross-governmental information monitoring, assessment and sharing model consisting of 10 government institutions, as well as develop a strategy on strategic communication in the field of national security.

Source: State Security Department of Lithuania (2022[9]), Threat Assessment, https://www.vsd.lt/en/threats/threats-national-security-lithuania/; Government of the Republic of Lithuania (2023[10]), "Lithuania's new crisis management model presented at Baltic States Centres of Government Meeting", https://lrv.lt/en/news/lithuanias-new-crisis-management-model-presented-at-baltic-states-centres-of-government-meeting/.

Other countries have put in place national-level co-ordination bodies with a scope that focuses on detecting and characterising disinformation operations orchestrated by foreign agents. France's Service for Vigilance and Protection against Foreign Digital Interference (VIGINUM) (Box 4.5), Sweden's Psychological Defense Agency (Box 4.6) and the Global Engagement Center in the United States (Box 4.7) have mandates limited to the threat of foreign information manipulation and interference. In these cases, a clear distinction is made regarding the provenance (domestic/external) of disinformation threats. In addition, the French Ministry for Europe and Foreign Affairs has established a dedicated unit to monitor disinformation operations against the French diplomatic network.

Box 4.5. The Service for Vigilance and Protection against Foreign Digital Interference – France

The French Service for Vigilance and Protection against Foreign Digital Interference (VIGINUM) was created under the General Secretariat for Defence and National Security (SGDSN) by the Decree no. 2021-922 of 13 July 2021 which sets out its missions.

The task of this national agency is to detect and characterise, through the analysis of publicly available online content, foreign manipulation of online information that may affect core issues of national interest (territorial integrity, security, diplomacy, and the functioning of its institutions, etc.). It also analyses their effects and co-ordinates the protection of the State against such operations.

In this respect, VIGINUM supports the SGDSN in co-ordinating an inter-ministerial network of administrations and services with technical capabilities in the field of information manipulation and foreign digital interference. It works closely with services and administrations contributing directly or indirectly to the fight against manipulation of information to detect and investigate malign operations. When malign operations are detected, the open-source investigation of VIGINUM supports counter-measures through the use of public communication aimed at restoring public trust, engaging with other ministries (including the Ministry of Europe and Foreign Affairs, Ministry of the Interior, Ministry of the Armed Forces, etc.) and with the authorities responsible for the smooth running of elections during electoral periods. Based on the investigation of VIGINUM, France has also publicly exposed multiple foreign digital interference campaigns

At the international level, VIGINUM engages in regular exchanges with international counterparts, both bilaterally and within the context of multilateral frameworks, such as the Rapid Alert System and the G7 RRM.

A fundamental element of VIGINUM is that it operates within a rigorous legal and ethical framework, notably defined by the Decree no. 2021-1587 of 7 December 2021. The latter is the result of consultations with parliamentary representatives and legal work with the French Council of State, based on its authorisation to consult, collect, and use, in an automated way, personal data publicly available online. The control of the management of the personal data collected online is supervised by the CNIL (the French National Commission for Information Technology and Civil Liberties). In addition, an ethical and scientific committee attached to the SGDSN has been set up to follow VIGINUM's activities. A representative of the highest French administrative court (the French Council of State) chairs the committee, which brings together qualified representatives from the fields of diplomacy, law enforcement, science, and media.

Source: SGDSN (2022[11]), Service de vigilance et protection contre les ingérences numériques étrangères "VIGINUM", https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques.

Box 4.6. The Swedish Psychological Defence Agency – Sweden

In January 2022, Sweden created the Swedish Psychological Defence Agency, a government agency under the Ministry of Defence that identifies, analyses and counters foreign malign information influence activities and other disinformation operations directed at Sweden or at Swedish interests.

The purpose of psychological defence is to safeguard Sweden's fundamental freedoms and independence through an open and democratic society and the free formation of opinion. The agency highlights that the government has a responsibility to ensure there is public awareness about information threats, without impinging on the freedoms of speech and expression. This preventive approach has a strong focus on critical thinking and education to build societal defences against disinformation, so that malign actors find a less favourable environment in which to conduct information influence activities.

The agency is organised in three departments: administration, operations, and capability development. In collaboration with other government agencies, its core tasks include:

- Producing reports and analysis relating to certain situations, threat actors, and societal vulnerabilities, as well as proposing relevant countermeasures.
- Developing methods and technologies for identifying and countering foreign malign information influence activities.
- Developing and strengthening Sweden's overall societal capability in terms of psychological defence. This includes providing support to the Swedish population, government agencies, municipalities, the media, voluntary defence organisations, and civil society, as well as enabling increased co-ordination between these actors.
- Supporting training exercises and knowledge development, for example initiating and funding research related to psychological defence.

Source: Swedish Psychological Defence Agency (2023[12]), Swedish Psychological Defence Agency website, https://www.mpf.se/en/about-us/.

Box 4.7. The Global Engagement Center – United States

The U.S. Department of State's Global Engagement Center (GEC), housed at the Department of State, was created in 2016 by Executive Order 13721. Its mission is to lead the U.S. government efforts to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States, its allies, and partner nations. The GEC pursues this mission in five areas:

- Analytics and Research: Analysts and data scientists at the GEC collect data from foreign state and foreign non-state actors to produce analysis on their malign information influence narratives, tactics, and techniques.
- International Partnerships: GEC has built and takes part in multiple international coalitions and partnerships with other national governments for the purpose of co-ordinating counter-disinformation analyses and actions, and collectively buttressing the integrity of the global information environment.
- Programmes and Campaigns: GEC tailors its initiatives to the specific challenges in unique overseas information environments and co-ordinates both internally within the Department, and with inter-

agency and international partners to build societal and institutional resilience to foreign propaganda and disinformation efforts abroad.

- Exposure: GEC plays a co-ordination role in inter-agency efforts to expose foreign information influence operations, including the use of proxy sites and social media networks overseas.
- Technology Assessment and Engagement: GEC identifies, assesses, and tests the use of technologies to counter foreign disinformation and propaganda abroad, and to reduce the risks posed by AI-generated media use in foreign malign actors' information manipulation overseas by sharing expertise among U.S. Government departments and agencies, and international partners.

Source: U.S. Department of State (n.d.[13]), "About Us – Global Engagement Center", https://www.state.gov/about-us-global-engagement-center-2/ (accessed on 31 August 2023).

The public communication function has also played a prominent role in co-ordinating efforts to respond to disinformation threats. Provided it has appropriate governance and sufficient resources, this function can play an important role in governments' efforts to strengthen their situational awareness of information threats and promote effective co-ordination of the response. To that end, the function should be grounded in efforts to promote the public good, should be undertaken transparently, and be guided by clear mandates that separate political and public communication activities. In that context, the French Ministry of Europe and Foreign Affairs has for instance run in 2023 and 2024 three public exposure campaigns based on investigations from VIGINUM with the publication of a technical report sharing the open sources data that helped French authorities draw the conclusions that Foreign digital interference had targeted the country.

The OECD Understanding Public Communication Survey from 2020 found that 64% of the 46 respondent countries indicated there were specific structures, teams, or individuals engaged in public communication efforts related to countering disinformation (OECD, 2021[14]). The focus on countering disinformation through the public communication function expanded rapidly during the COVID-19 pandemic, as governments sought to counter fast-spreading false narratives about the causes of the virus and medically unproven cures.

As it applies to public communication, centralised capacity can be useful in producing communal resources, sharing information, and developing a coherent public response for agencies and ministries at the national level. In the United Kingdom, the architecture of public communication responses has emerged as a result of interventions and approaches designed to tackle several waves of disinformation. For example, the Counter Disinformation Unit (CDU) leads ongoing actions to monitor and flag false and misleading content, either to prompt debunking or to liaise with online platforms. In addition, the Government Information Cell (GIC), which sits within the Foreign, Commonwealth and Development Office (FCDO), was set up on the eve of Russia's large-scale invasion of Ukraine with the mission of countering information operations by hostile actors that pose threats to UK security, foreign policy, and democratic institutions (OECD, 2023[15]).

Additional examples of such offices include those focused on implementing specific initiatives and policies designed to counter disinformation by strengthening the media and information space more broadly. This is the approach taken in Italy, for example, via the Department for Information and Publishing (see Box 4.8).

Box 4.8. The role of the Department for Information and Publishing in Italy

In Italy, the Department for Information and Publishing – seated within the Prime Minister's Office under the political responsibility of a Secretary of State – oversees the design and of the implementation of policies to support media freedom and pluralism both for traditional media (publishing houses, newspapers, and periodicals) and digital media, while enforcing copyright protection. Countering disinformation has become one of the defining objectives of the Department, as it is focused on guaranteeing a professional, independent, and diverse information ecosystem and the free flow of trustworthy information.

One of the Department's main activities is to provide financial support to professional media to foster information pluralism (see Chapter 2). Financial sustainability is a pressing challenge for quality journalism, as both traditional and digital-first publishers face severe financing constraints. The new Single Fund for Pluralism and Digital Innovation in the Information and Media Publishing Sector replaces all previous permanent and one-off facilities and mainstreams public financial support to the media ecosystem. The aim of this effort is to strengthen information quality and reliability, and to provide incentives to increase the number of professional journalists, including through innovative media products and investments in new content and new technology.

The Department for Information and Publishing also supports the implementation of the National Cybersecurity Strategy (2022-2026). As the national co-ordinator of the measure to prevent and fight online disinformation, the Department focuses on two projects: a) strengthening citizens' media literacy, including through information campaigns on possible harmful uses of artificial intelligence; and b) developing in-depth knowledge of the relevant threats, in partnership with universities, to issue guidelines to support the public communication function.

In addition, the Department has set up a Committee of Experts with the task of analysing the impact of generative AI in the information and publishing sector. The Committee's 2024 report highlights the perceived risk that artificial intelligence poses to the spread of disinformation; the broad support for establishing stable multi-stakeholder alliances for reliable and quality information sharing between citizens, public institutions, and the media; the need to protect the employment of journalists and to defend the sector's professionalism; and recommendations to protect the democratic space from foreign interference and manipulation by malign actors.

Source: Article 1 § 315 of the Law No. 213 of 2023 (Budget Law for 2024); Article 17 of the Decree Law No. 198 of 2022 converted into Law No. 14 of 2023 and Decree of the President of the Council of Ministers of 11 July 2023; Measure #24 of the National Cybersecurity Strategy Implementation Plan; Decree of the Undersecretary of State responsible for information and publishing of 23 October 2023.

Task forces and working groups

In addition to establishing central units to co-ordinate responses to disinformation, governments can also consider putting in place task forces composed of officials from across the public service or external partners to advise policy responses. These task forces can be either permanent or temporary in nature. It is important to note that different expert units can be set up within the same country, which may allow for more responsive interventions and technical work when specific objectives are at stake.

Germany has followed a specific configuration, with one ministry directing national policy to disinformation, complemented by a network of inter-ministerial task forces and working groups co-operating on specific thematic priorities (Box 4.9).

Box 4.9. Inter-ministerial working groups to counter disinformation – Germany

Within Germany's Federal Government, the Federal Ministry of the Interior and Community (BMI) has a strategic co-ordinating role in relation to disinformation threats. Germany has also set up special working groups that bring together officials from different ministries at the national and federal level and intelligence services.

The BMI chairs an inter-ministerial working group on hybrid threats created in 2018 to deal with the manipulation of public opinion via the spread of disinformation and propaganda online, espionage and cyber-attacks on critical infrastructures, among other threats.

When Russia's war of aggression against Ukraine began, a special task force within this working group was created to focus on Russian disinformation. The BMI together with the Federal Foreign Office (AA), the Press and Information Office of the Federal Government and national intelligence services carefully monitor the information space to identify Russian narratives. They also invest efforts in reinforcing pro-active and fact-based communication, providing updates on the situation and encouraging a more critical approach to information and sources, particularly those in social media. The BMI focuses on disinformation orchestrated by foreign states or actors to influence public opinion and strives to strengthen societal resilience. The Federal Government also engages in regular and intensive discussions with international partners, both bilaterally and in the context of the European Union, G7, and NATO.

Source: Federal Ministry of the Interior and Community (2023[16]), "Measures taken by the Federal Government to fight disinformation", https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation/measures-taken-by-the-federal-government.html.

In Chile, a "National Commission Against Disinformation" was set up in 2023 as an advisory committee to provide counsel to the Ministry of Science, Technology, Knowledge, and Innovation and the General Secretariat of Government (*Segegob*) on the effects of disinformation on democratic quality of digital platforms, digital literacy, and good digital practices (Box 4.10).

Box 4.10. Chile's National Commission Against Disinformation

Chile's National Commission Against Disinformation, located within the Ministry of Science, Technology, Knowledge and Innovation, was created by official decree in May 2023. The aim of this temporary body is to provide advice to the Minister of Science, Technology, Knowledge, and Innovation, and the Minister Secretary General of Government, on matters related to the global phenomenon of disinformation and its manifestation in Chile. The commission is composed of 9 members representing state and private universities, NGOs, foundations and fact-checking organisations. The Commission is tasked with delivering two reports within one year: the first to examine disinformation threats, and the second to provide guidelines and recommendations for the formulation of relevant public policies.

Source: Ministry of Science, Technology, Knowledge and Innovation (n.d.[17]), "Comisión Asesora contra la Desinformación", https://www.minciencia.gob.cl/areas/comision-contra-la-desinformacion/.

Countries have also set up regular consultations and assessments to ensure that policy responses are adapted to developments in the information space. For instance, Canada's Protecting Democracy Unit at the Privy Council Office recently established an inter-departmental group to identify policy gaps in the Government of Canada's approach to disinformation, and an interdepartmental research co-ordination group to ensure well aligned and comprehensive research efforts on the topic.

Finally, even where countries have not established a cross-government co-ordination mechanism dedicated to counteracting disinformation or building information integrity generally, governments may establish task forces bringing together different offices, such as the Centre of Government (Cabinet Office or Office of the Presidency) and ministries or departments of foreign affairs, strategic communications, health, education, culture, defence, and digital policies, particularly when responding to specific thematic priorities. For example, in 2023, Brazil established an inter-ministerial Committee to Combat Disinformation related to the National Immunization and Public Health Policies. The aim of the Committee is to provide a strategic and integrated approach to support the Ministry of Health in developing and evaluating public communication around health issues, exchange information across the government on disinformation related to the public health policies, and develop relevant research, resources, and trainings to support the government's efforts to counteract disinformation in this space. The Committee includes representatives from the Secretariat of Social Communication of the Presidency of the Republic, the Attorney's-General office, the Comptroller General, the Ministry of Science, Technology and Innovation, the Ministry of Justice and Public Security, and the Ministry of Health (Government of Brazil, 2023[18]).

Country experiences in establishing co-ordination mechanisms to-date suggest that governments are increasingly appreciating the value of organised and coherent efforts to counter disinformation threats and enhance information integrity. The initiatives also highlight the importance that the offices do not contribute to politicisation or facilitate speech restrictions, while at the same time enabling efficient and timely dissemination of intelligence between relevant authorities (including at the local, federal, and national level) and, potentially, external partners. Efforts to ensure robust and sustainable functioning of the co-ordination mechanisms also point to the importance of setting clear mandates, including by defining the disinformation threat(s) the mechanism or office seeks to address.

4.2.3. International co-ordination and co-operation is essential in the fight against disinformation

As information flows know no borders in today's globalised and digitalised world, international co-operation and co-ordination is a critical element to design policy responses at the level of the information integrity challenge. The transnational nature of this challenge is also visible in the use of information manipulation by foreign malign actors to interfere in national affairs; failing to engage in transnational dialogues could lead hostile states to use a fragmented approach to their advantage (Pamment, 2020[19]). False and misleading information can also have negative effects across borders on issues related to public health, minority communities, and climate change (Lewandowsky, 2021[20]; UNDP, 2021[21]). In this context, as for other areas of the digital economy, international regulatory co-operation should be part of the policy toolbox aimed at responding to disinformation threats and reinforcing information integrity.

Countries are therefore collaborating and co-ordinating their actions internationally to reinforce their ability to counteract these threats. Indeed, national responses are most effective when they are informed by other countries facing similar problems and can draw on relevant lessons. Enhancing domestic co-ordination will therefore facilitate countries' efforts to participate and engage in international initiatives whose mission is to prevent and counter disinformation activities (Jeangène Vilmer, 2021[22]).

There are multiple international fora and co-ordination mechanisms, each presenting different configurations of country alliances and thematic priorities. International organisations, specialised or ad hoc groups, and government-led convenings and framework agreements account for the primary methods by which countries engage on these issues bilaterally and multilaterally. Despite the range and diversity of international co-ordination options, 90% of survey respondents indicated that strengthening co-

operation with partner countries is a priority area for improvement when it comes to tackling disinformation threats.[5]

First, international organisations are continuing to build their efforts to support countries in reinforcing information integrity. For example, in addition to the OECD's DIS/MIS Resource Hub,[6] which serves as a platform for policy analysis and dialogue among the 38 Member countries and beyond, the OECD brings together Member and non-member countries via a range of initiatives and networks. These initiatives focus on issues such as artificial intelligence,[7] the exploration and promotion of more effective governance for information integrity in developing countries,[8] and transparency reporting by online platforms.[9] Together, these OECD initiatives help inform the work of the OECD DIS/MIS Resource Hub and the global effort to reinforce information integrity.

The NATO Secretariat and the NATO Strategic Communications Centre of Excellence (NATO StratCom COE, established in Latvia in 2014), conduct analysis, research, and support strategic communication responses to the spread of disinformation. EUvsDisinfo[10] is a project of the European External Action Service's East StratCom Task Force established in 2015 with the aim to better forecast, address, and respond to Russian disinformation campaigns affecting the European Union, its Member States, and other countries in the region (the EU's trans-national regulatory impact is discussed further in Chapter II). Finally, the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) was established in Finland in 2017 to counter hybrid threats and build capacity and awareness in participating countries (Box 4.11).

Box 4.11. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)

An international hub of experts to optimise analytical capabilities and training opportunities

The Hybrid CoE was established in 2017 by the first nine participating states, NATO, and the European Union in Helsinki. The motivation for its creation was to develop resilience and build capacity to counter hybrid threats through research and practical training and exercises involving participants from private, public, civil, military and academic sectors. Today, Hybrid CoE counts 33 participating states.

The term hybrid threat can be defined as an action conducted by state or non-state actors to undermine or harm democratic governments by influencing decision-making. These threats combine military and non-military, as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, migration, deployment of irregular armed groups and use of regular forces. Such actions are co-ordinated and synchronised, using a variety of means and designed to remain below the level of detection and attribution (NATO, 2023[23]).

The Hybrid CoE is actively involved in a wide range of educational projects and training exercises. In 2022, they organised the Helsinki Countering Disinformation Wargame, a hybrid threat simulation game focused on Russian and Chinese disinformation designed to help identify gaps and strengths in the resilience systems of countries. The aim of these real-word simulations is to further develop tools and techniques to counter disinformation and strategic communication plans tailored to Hybrid CoE's participating states needs and threat landscapes.

Source: Hybrid CoE (n.d.[24]), "What is Hybrid CoE?", https://www.hybridcoe.fi/about-us/.

For its part, UNESCO supports its global membership in developing media and information literacy activities and enhancing the capacity of policymakers, educators, journalists and media professionals, youth organisations, and disadvantaged populations.[11] Additionally, UNESCO has developed Guidelines for Regulating Digital Platforms, a high-level document that aims to "safeguard freedom of expression and access to information and other human rights in digital platform governance, while dealing with harmful content that can be permissibly restricted under international human rights law and standards online (UNESCO, 2023[25])." Also within the UN system, the United Nations Development Programme (UNDP) explores information integrity as it relates to UNDP's mandate and thematic areas of focus. At the programmatic level, UNDP provides practical guidance for programme design.[12]

Beyond broad-based member engagement via international organisations or the European Union, governments have established more targeted engagement mechanisms to tackle aspects of the fight against disinformation. The United States recently unveiled a new tool to build international consensus around a common approach to foreign disinformation and information manipulation and protect free and open societies (see Box 4.12 for additional information).

Box 4.12. The Framework to Counter Foreign State Information Manipulation – U.S. Department of State

The Framework to Counter Foreign State Information Manipulation was announced by the U.S. Department of State in January 2024 and is being implemented by the Global Engagement Center. It seeks to develop a common understanding of this threat and deepen co-operation between like-minded partners, establish a common operating picture, and support the development of resilient, fact-based information ecosystems. It fosters alignment along a common set of action areas to enable the development of co-ordinated responses to foreign information manipulation. It includes five key action areas:

1. National Strategies and Policies
2. Governance Structures and Institutions
3. Human and Technical Capacity
4. Civil Society, Independent Media, and Academia
5. Multilateral Engagement

By committing to these five key action areas, international partners can improve bilateral and multilateral cohesion to build societal resiliency to foreign disinformation and information manipulation.

Source: U.S. Department of State (2024[26]), "The Framework to Counter Foreign State Information Manipulation", https://www.state.gov/the-framework-to-counter-foreign-state-information-manipulation/.

At the G7 level, for example, the Rapid Response Mechanism (G7 RRM) constitutes a mechanism to strengthen co-ordination to identify and respond to diverse and evolving foreign threats to democracy. Created in 2018, it comprises Focal Points from G7 Members, and includes the European Union, NATO, Australia, New Zealand, the Netherlands, and Sweden as observers (see Box 4.13).

Box 4.13. The G7 Rapid Response Mechanism

The G7 Rapid Response Mechanism (G7 RRM) was established by Leaders at the 2018 G7 Summit in Charlevoix. Global Affairs Canada's Rapid Response Mechanism Canada (RRM Canada) team serves as its permanent secretariat. The G7 RRM mission is to strengthen co-ordination between G7 countries to identify and respond to diverse and evolving foreign threats to democracy, including by focusing on strengthening the media and information environment; responding to foreign threats to the rights and freedoms of citizens; and promoting elections security. The G7 RRM Focal Points meet monthly to share information, best practices, and lessons learned.

Source: Rapid Response Mechanism Canada: Global Affairs Canada, https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/index.aspx?lang=eng.

The Lublin Triangle was put in place by Poland, Lithuania, and Ukraine to establish trilateral co-operation to counter Russian disinformation campaigns. These three countries have worked together to identify specific narratives, messages, and tactics used against them; analyse the degree of societal resilience to Russian government propaganda; and make recommendations to better address evolving threats (Box 4.14).

Box 4.14. The Lublin Triangle – Trilateral co-operation to tackle Russian disinformation

In July 2020, the Ministers of Foreign Affairs of Poland, Lithuania, and Ukraine established the Lublin Triangle (L3), a regional initiative to strengthen mutual military, cultural, economic, and political co-operation based on historical ties and traditions. In 2021, the L3 countries signed a Roadmap setting the key directions of expanding the co-operation, including joint strategic activities to respond to hybrid threats, counteract disinformation, and strengthen societal resilience. The work of the Lublin Triangle is guided by a Joint Action Plan to Combat Disinformation for 2022-2023.

Source: Instytut Kościuszki (2022[27]), Report – Resilience to Disinformation, https://ik.org.pl/en/.

Governments have also established a range of convenings and frameworks that provide platforms for discussion, establish priorities moving forward, and set a common direction for action. For example, the United States established and hosted the first two meetings of the Summit for Democracy (in December 2021 and March 2023, respectively), with the third hosted by the Republic of Korea in March 2024. Around 100 governments participated in the first two Summits, and a theme of the 2023 Summit for Democracy focused on Information Integrity, with specific attention paid to issues around international co-operation, information literacy, and definitions.[13]

Building directly on the work of the Summit for Democracy's Cohort on Information Integrity, the Governments of Canada and the Netherlands launched the Global Declaration on Information Integrity Online in September 2023. This declaration "lays out a set of high-level international commitments to protect and promote information integrity online…and seeks to strengthen existing multilateral efforts to protect the information ecosystem (Government of the Netherlands, 2023[28])" (see Box 4.15).

Box 4.15. The Global Declaration on Information Integrity Online

The Global Declaration on Information Integrity Online, launched in September 2023 and signed by 34 countries, lays out international commitments by participating states to protect and promote information integrity online. It also sets out expectations for the private sector and online platforms to employ business practices that contribute to a healthy information ecosystem online. The Declaration is endorsed by: Australia, Austria, Belgium, Brazil, Canada, Chile, Costa Rica, Czechia, Denmark, Dominican Republic, Estonia, Finland, France, Germany, Georgia, Iceland, Ireland, Japan, Kenya, Latvia, Lithuania, Luxembourg, Moldova, Netherlands, New Zealand, North Macedonia, Republic of Korea, Slovak Republic, Sweden, Switzerland, United Kingdom, Uruguay, and United States.

The Declaration defines the term "information integrity" as an information ecosystem that "produces accurate, trustworthy, and reliable information, meaning that people can rely on the accuracy of the information they access while being exposed to a variety of ideas."

Specific commitments made by participating states include:

- Abstaining from and condemning state-led disinformation campaigns
- Respecting, promoting, and fulfilling the right to freedom of expression
- Implementing relevant legislation in compliance with international law
- Avoiding stifling freedom of expression under the guise of countering disinformation
- Promoting stronger civic education online and digital literacy
- Supporting independent media, news, and journalism
- Taking active steps to address disinformation targeting groups in vulnerable situations.

The Declaration also calls on online platforms and the industry to play a constructive role by respecting the rule of law, human rights, and fundamental freedoms; promoting research; enhancing transparency; enhancing oversight of algorithms; and preserving election and democratic integrity.

Source: Government of the Netherlands (2023[29]), Global Declaration on Information Integrity Online, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2023/09/20/global-declaration-on-information-integrity-online.

Another example of a platform for multi-lateral discussion is the EU-US Trade and Technology Council (TTC), which was established in 2021 to serve as a forum for the United States and European Union to co-ordinate on global trade, economic, and technology issues. At the fourth Ministerial meeting of the TTC in May 2023, the Joint Statement noted the shared "deep concern regarding foreign information manipulation and interference (FIMI) and disinformation." It also flagged the "opportunity to develop a shared standard for threat information exchange on FIMI" and included a call to "enhance the preparedness of the multi-stakeholder community to step up their actions against FIMI threats, including by exploring further support for capacity building in Africa, Latin America, and EU Neighbourhood countries (TTC, 2023[30])."

The International Partnership on Information and Democracy is an intergovernmental non-binding agreement endorsed by 52 countries to promote and implement democratic principles in the global information and communication space (see Box 4.16). Oversight and implementation of the Partnership is co-ordinated by the Forum on Information and Democracy, which is an independent non-profit entity led by civil society organisations. Mandating the Forum to serve as an independent civil society group to support the Partnership provides important engagement opportunities for government and non-government partners to benefit from experts and scholars convened to evaluate the global information and communication space, as well as to develop recommendations to the different stakeholders that shape how norms should evolve (Forum on Information and Democracy, 2023[31]).

Box 4.16. International Partnership for Information and Democracy

Signed during the 74th UN General Assembly in September 2019, the International Partnership for Information and Democracy affirms the following principles:

1. The global information and communication space, which is a shared public good of significant democratic value, must support the exercise of human rights, most notably the right to freedom of opinion and expression, including the freedom to seek, receive and impart information and ideas of all kinds, through any media of one's choice regardless of frontiers, in accordance with the International Covenant on Civil and Political Rights (Article 19).
2. Access to reliable information must be protected and promoted to enable democratic participation and the exercise of freedom of opinion and expression.
3. Information can be regarded as reliable insofar as its collection, processing and dissemination are free and independent, based on cross-checking of various sources, in a pluralistic media landscape where the facts can give rise to a diversity of interpretation and viewpoints.
4. In accordance with the international law and standards on the right to freedom of opinion and expression, journalists and media workers, in the course of their function, must be protected against all forms of violence, threats, and discrimination; against all forms of arbitrary detention, abusive legal proceedings; against any unduly restrictive efforts to prevent them from carrying out their works and have access to appropriate legal remedies, including as relevant with respect to the confidentiality of their sources.
5. Sustainable business models must be developed to serve high-quality independent journalism.

Source: Forum on Information & Democracy (n.d.[32]), "International Partnership for Information & Democracy", https://informationdemocracy.org/international-partnership-on-information-democracy/.

Notably, these examples do not include bi-lateral engagements or international co-operation focused on intelligence or security issues. Countries have noted, however, that they engage in these networks and initiatives to benefit from timely information sharing, cross-fertilise research, engage in capacity building activities and the exchange of best-practices, and clarify directions for shared action. These mechanisms are also key to developing common terminology, sharing strategic intelligence and analytical methodologies, enhancing research, and overcoming domestic political divides.

Moving forward, governments and international organisations alike will need to continue to respond to new and emerging issues in the information space while avoiding overlapping with or duplicating other initiatives (see, for example the OECD Recommendation on International Regulatory Co-operation to Tackle Global Challenges (OECD, 2022[33])). More needs to be done to ensure a clear focus on taking advantage of the opportunities provided by unique perspectives, membership, and mandates of relevant organisations and to co-ordinate shared global action.

4.3. CHANGES WITHIN THE INFORMATION SPACE REQUIRE A GREATER FOCUS ON BUILDING CAPACITY IN THE PUBLIC ADMINISTRATION

Building collective government capacity to help address the challenges posed by disinformation starts with the public officials who confront these threats in their daily work. The level of sophistication of disinformation campaigns requires upskilling and training at all levels of government to ensure that elected officials and policymakers have the knowledge and tools to recognise, monitor, and counter the spread of false and misleading information without impinging on human rights and fundamental freedoms. Capacity building efforts should also be designed with the wider aim of encouraging critical thinking and increasing public

officials' awareness about the risks of disinformation. This is also important to help prevent them from spreading false narratives. To that end, involving national schools of public administration or specialised offices, such as the Belgian Integrity Bureau, may help ensure the capacity building efforts in this space reinforce the broader aims of reinforcing information integrity and building citizen trust.

According to the OECD survey, 90% of responding countries indicated that building the capacity of public officials to track and respond to disinformation threats is a priority for the future. At the same time, however, only 65% reported having regular and specialised training on countering disinformation. For instance, in Colombia, the Ministry of Information and Communication Technologies (MinTIC) has taken proactive steps to train its Press Office team. Those who join the Press Office team receive training on how to identify possible disinformation narratives and to better react to these situations. The Dutch Ministry of the Interior and Kingdom Relations, for its part, drafted a "Guidance on dealing with disinformation" in 2022 to provide civil servants with general guidance (see Box 4.17).

Box 4.17. Guidance on dealing with disinformation – The Netherlands

In January 2022, the Dutch Ministry of the Interior and Kingdom Relations drafted a "Guidance on dealing with disinformation," which provides public officials with an overview of how false and misleading information can be spread and recognised; the mechanics of polarisation in the information space; and legal and practical advice on how to minimise the impact of disinformation and what they can do if confronted with it. The guidance is structured around four main themes:

1. Overview of disinformation risks and effects: This section reiterates media and information literacy skills of verifying sources and content; it also provides an overview of the societal risks of disinformation, including that purposefully false and misleading content can exacerbate polarisation and undermine trust in democracy.
2. Preparing: This section presents an overview of the importance of establishing effective organisational structures; communicating with the media and the public to build media and information literacy; and establishing effective and proactive public communication initiatives.
3. Responding to disinformation: This section presents an overview of how communicators should decide how best – or even whether – to respond to particular narratives, as well as examples of effective messages.
4. Legal options: This section reiterates that the government must always act within the constitutional framework of freedom of expression and that disinformation content cannot simply be restricted; it also lays out the legal framework that informs illegal content and harms caused by the spread of false or misleading content.

Source: Jahangir (2023[34]), *Disinformation Landscape in the Netherlands*, https://www.disinfo.eu/wp-content/uploads/2023/09/20230919_NL_DisinfoFS.pdf; Ministry of the Interior and Kingdom Relations (2022[35]), Handreiking omgaan met desinformatie, https://www.weerbaarbestuur.nl/sites/default/files/inline-files/BZK%20-%20Handreiking%20omgaan%20met%20desinformatie.pdf.

Another example is the UK's RESIST 2 Toolkit, which is used in trainings to help government officials build individual and societal resilience to disinformation through strategic communications (Box 4.18).

Box 4.18. United Kingdom's RESIST Counter-Disinformation Toolkit

In 2018, the UK government, in consultation with civil society and partner countries, developed the RESIST framework, a step-by-step approach to countering disinformation that helps deal with the challenge in a systematic and efficient way, while ensuring that core democratic principles such as freedom of expression are protected. RESIST stands for Recognise mis- and disinformation, Early warning, Situational insight, Impact analysis, Strategic communication, and Tracking effectiveness.

This framework was translated into a public toolkit with the primary aim of giving professional communicators and citizens confidence in assessing the veracity of information. Since the publication of RESIST in 2019, the UK government has trained over five hundred communicators from at least 20 partner countries through a mixture of in-person training, remote sessions and digital learning.

Since the original RESIST framework, communications professionals and civil servants from the United Kingdom and around the world have provided feedback about how they use the toolkit, and what they would like to see in future iterations. This is why in 2021 the UK government published the RESIST 2 Counter-Disinformation Toolkit an updated version that reflects both the changing demands of the communication profession, and the evolving information environment exploring new techniques and tactics.

Source: UK Government Communication Service (2021[36]), RESIST 2 Counter Disinformation Toolkit, https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/.

Capacity building programmes should also be closely connected with the latest available research. Partnering with organisations active in the field of information integrity can therefore help ensure the provision of high-quality, innovative and cost-effective learning opportunities. Public officials in Italy, for example, benefit from trainings informed by research from the European Digital Media Observatory, an independent centre of expertise that promotes scientific knowledge on online disinformation, encourages the development of fact-checking services, and supports media literacy projects (see Box 4.19 – additional information on engaging with non-governmental partners can be found in Chapter III).

Box 4.19. Ministry of Foreign Affairs training on disinformation and strategic communication – Italy

The Italian Ministry of Foreign Affairs (MFA) provides training on disinformation and strategic communication as part of its capacity building efforts for diplomats, public servants in Italian Cultural Institutes, and military personnel to be deployed abroad. The MFA also supported the creation of an Italian national hub to combat disinformation – the Italian Digital Media Observatory (IDMO), an EU-funded project that promotes scientific knowledge on online disinformation, encourages the development of fact-checking services and supports media literacy programmes. IDMO works with embassy representatives and key interlocutors such as RAI, the LUISS School of Journalism and Newsguard, among others.

The Italian Ministry of Foreign Affairs also produces communication products and co-ordinates social media campaigns to raise public awareness of disinformation, such as a special episode of the podcast "Voci dalla Farnesina" (Voices from the Farnesina), which featured journalists, academics and diplomats to discuss differences in terminology between misinformation, disinformation and malinformation and to encourage citizens to think critically about the industry of information manipulation on digital platforms.

Source: Italian Digital Media Observatory (n.d.[37]), "Uniti contro la disinformazione", https://www.idmo.it/.

Canada has also invested in training for civil servants focused on cultivating an understanding of and resilience to disinformation by adapting the UK's RESIST 2 Toolkit to the Canadian context (Box 4.20).

Box 4.20. Privy Council Office counter-disinformation training – Canada

Canada has approached building understanding of and resilience to disinformation in the Canadian context by promoting an informed and engaged citizenry, including its public servants. With an annual budget of CAD 2 million, the Protecting Democracy Unit at the Privy Council Office co-ordinates, develops, and implements government-wide measures designed to combat disinformation. This includes the Countering Disinformation: A Guidebook for Public Servants, which offers guidance on how to navigate the threat of mis- and disinformation, building upon the United Kingdom's RESIST model. Canada's School of Public Service also combines face-to-face training via hybrid courses, covering topics such as research on the behavioural drivers of misinformation and trust in institutions, and the use of social media platforms for public communication.

Source: Government of Canada (2022[38]), "Backgrounder: Government of Canada to fund projects addressing the growing problem of online mis/disinformation", https://www.canada.ca/en/canadian-heritage/news/2022/07/backgroundergovernment-of-canada-to-fund-projects-addressing-the-growing-problem-of-online-misdisinformation.html; Government of Canada (n.d.[39]), "Countering Disinformation: A Guidebook for Public Servants", https://www.canada.ca/en/democratic-institutions/services/protecting-democratic-institutions/countering-disinformation-guidebook-public-servants.html; Government of Canada (2023[40]), "The Trust Series: Trust and Misinformation in Digital Information Ecosystems (TRN1-E11)", https://catalogue.csps-efpc.gc.ca/product?catalog=TRN1-E11&cm_locale=en; Government of Canada (2022[41]), "Navigating Social Media as a Public Servant (TRN125)", https://catalogue.csps-efpc.gc.ca/product?catalog=TRN125&cm_locale=en.

Countries' experiences with capacity building on this topic point to the importance of developing public officials' knowledge of and skills to track and counter disinformation. Examples of capacity building efforts point to the value of designing evidence-based and accessible programmes that consider cultural and linguistic sensitivities and that are delivered in multiple formats, including offline and online, workshops, toolkits, and handbooks. Experience also points to the value of encouraging mobility of personal across agencies and offices so that they leverage expertise among projects and peers.

4.4. GOVERNMENTS WILL NEED TO CONTINUE TO DEVELOP AGILE REGULATORY GOVERNANCE TO BUILD INFORMATION INTEGRITY

Regulation is an essential tool for governments to build information integrity, respond to the threat of disinformation, and to achieve the societal aims of reinforcing democracy more broadly. Nevertheless, key questions remain around what strategies to pursue and how best to approach the act of regulating. Considerations include the processes and institutions that are put in place to design, enforce, and review regulation (OECD, 2018[42]). This is further captured by the OECD Recommendation of the Council on Agile Regulatory Governance (OECD, 2021[43]).

More recently, the OECD launched the *Better Regulation in the Digital aGE (BRIDGE)* initiative, which seeks to support countries in implementing effective regulatory governance for digital activities. When approached from the "better regulation" perspective, it highlights how regulation has the power to effectively manage risks associated with digital technologies, while also promoting digital innovation. However, the pace of technological change, existing regimes that lack agility in the digital world, new activities and business models, and the global nature of digital activities are putting limits on governments' abilities to effectively reinforce information integrity.

Moving forward, considerations related to regulatory policy should focus on, as appropriate:

- Fostering a more agile regulatory governance approach to regulating in the information space
- Clarifying enforcement approaches for regulation related to information integrity.

4.4.1. Fostering a more agile regulatory governance approach to regulating in the information space

Particularly in the rapidly evolving information space, regulatory policy should be designed to be agile and responsive to the challenges brought by digitalisation and emerging technologies. Whereas traditional regulation is often designed on an issue-by-issue, sector-by-sector, or technology-by-technology basis, digital and emerging communication technologies often erode, straddle, or blur the usual delineations. Digital and emerging technologies also blur the traditional distinction between consumers and producers (Amaral et al., 2020[44]).

The traditional notion of liability is therefore often insufficient as it relates to responding to mis- and disinformation, given that the risks to those affected, the technologies used, and the origins of such content may all be in different jurisdictions. The erosion of the usual delineation of markets undermines the relevance of regulators' traditional mandates and remits; new ways of communicating and engaging pose challenges to enforcement of existing rules; fragmentated approaches across jurisdictions prevent consistent and co-ordinated approaches despite the cross-border effects of many information and communication technologies; and the mismatch between the pace of technological development and that at which regulatory frameworks evolve (the "pacing problem") all pose new and challenging issues for governments and regulators (Amaral et al., 2020[44]).

Given the regulatory challenges raised by the complexity of the information space, undertaking a shift in regulatory policy processes will be essential. As noted by the OECD Recommendation on Agile Regulatory Governance to Harness Innovation, "the traditional 'regulate and forget' mindset must give way to 'adapt-and-learn' approaches. A more agile approach to regulatory policymaking will help ensure governments have the capability to understand innovations and their potential impact on existing regulations and public values more broadly (OECD, 2021[45]). In the information space, regulatory agility should be directed at understanding the intended (and unintended) effects of existing regulation, as well as applying lessons to new technologies such as generative AI.

Utilising proper management tools to effectively design, implement, and evaluate regulations will be important in this regard. For example, putting in place mechanisms for public and stakeholder engagement in the regulatory process, including citizens, small and medium-sized enterprises, and start-ups, from an early stage and throughout the policy cycle can help enhance transparency, build trust, and capitalise on diverse sources of expertise. Carrying out regulatory impact assessments (RIA) that assess all relevant policy options, including non-regulatory alternatives, is also crucial, as is putting in place comprehensive RIA processes and outlining subsequent evaluation (see Box 4.21 for an overview of the Impact Assessment Report of the DSA). Finally, monitoring the impact of regulations systematically and continually, engaging in timely and proportionate re-evaluation, and embedding review requirements in appropriate frameworks will all help contribute to agile regulation (OECD, 2021[45]).

Box 4.21. The EU Digital Services Act Impact Assessment Report

The DSA Impact Assessment Report notes that the regulation builds on the evaluation of the E-Commerce Directive from 2000 and that it seeks to respond to three core problems driving the regulation, including: that citizens are exposed to increasing risks online, and particularly on very large online platforms; that the supervision of online platforms is largely uncoordinated and ineffective in the European Union; and that national-level regulations risk leading to increasing barriers in the internal market and reinforcing competitive advantages for established very large platforms and digital services.

The Impact Assessment Report also noted that anticipated benefits of the DSA would be to boost competitiveness, innovation, and investment in digital services, while targeting specific harms. Furthermore, the regulation will seek to promote transparency and safety online, as well as protect fundamental rights. Enhanced co-operation between Member States and the EU level governance will improve enforcement and provide an up-to-date supervisory system for digital services. Notably, the Impact Assessment Report also notes that revision should take place within five years of the entry into force, and that regular reports would be part of the design of the supervisory system.

Source: European Commission, Brussels, 15.12.2020 SWD(2020) 349 final, Executive Summary of the Impact Assessment Report Accompanying the document: Proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC.

That said, addressing the rapid pace of technological progress requires shortening timeframes throughout the policymaking process and using regulatory management tools in a more dynamic manner. To help promote more agile and flexible regulation, these policy processes – public engagement, conducting regulatory impact assessments (RIA), monitoring, and *ex post* evaluation – should "not be undertaken as a series of discrete requirements to be conducted successively, but rather as mutually complementary tools embedded in the policy cycle to inform the appropriate adaptation of regulatory (or alternative) approaches (OECD, 2021[45])." Ensuring the flexibility and proportionality of regulation should be backed by government institutions that protect the rights of stakeholders and give them access to redress mechanisms if these rights are violated (OECD, 2018[46]).

The pace and breadth of change also requires a more anticipatory regulatory approach grounded in institutional capacity and mechanisms to better understand how emerging technologies may affect societies, markets, and government actions. Notably, such an effort will require establishing constructive partnerships with non-governmental partners to facilitate greater understanding of – and more effective responses to – the challenges to information integrity brought by technological development (OECD, 2022[47]). Governments should also increase the capacity of oversight and advisory bodies to anticipate and implement strategic foresight that informs the design, implementation, and analysis of regulations. Building capacity requires devoting appropriate resources to develop the necessary skills around conducting impacts assessments, building strategic foresight, as well as understanding the costs and benefits of innovation and new technologies (OECD, 2021[43]).

Experimentation, including in the form of regulatory sandboxes, can help to render frameworks more adaptive through ongoing learning and adjustment. It can also help to reduce uncertainty levels surrounding decision-making, particularly in situations where sufficient reliable information on potential impacts or effectiveness of regulatory options cannot be obtained through traditional approaches, such as information gathering and consultations. Similarly, it can serve to enhance the evidence base that can help inform the revision of existing regulation or inspire new rules.

Finally, in an increasingly inter-connected world, co-operation among governments and policymakers across jurisdictions is essential to ensure the effectiveness, coherence, and continued relevance of regulatory policies and frameworks. To this end, international regulatory co-operation (IRC) is critical to avoid fragmentation and prevent regulatory arbitrage, or the effort to take advantage of differences between

systems to avoid more burdensome regulation (OECD, 2012[48]). Moreover, considering the substantial resource needs associated with regulating the information space, IRC can help governments and regulators target and use those resources as efficiently as possible.

4.4.2. Enforcement considerations for regulation in the information space should be clarified

Regulations in this space cannot achieve their stated objectives unless actors comply and the requirements are properly enforced. To do so, countries should consider implementing a range of strategies and mechanisms to ensure compliance, including a combination of monitoring actions by oversight bodies, oversight by third-party auditors, and the provision and application of sanctions. Integrating these enforcement-related considerations in legislative proposals and related assessments can help provide clarity and direction.

These considerations include data and information requirements to verify compliance, as well as institutional and cross-border co-operation initiatives built into the use of regulatory management tools (OECD, 2021[45]). For example, the DSA requires the Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) to "assess the systemic risks stemming from the design, functioning and use of their services, as well as from potential misuses by the recipients of the service, and should take appropriate mitigating measures in observance of fundamental rights" and be proportionate in their mitigation measures (DSA, Rec. 79 and Art. 34) (European Union, 2022[49]). Notably, the DSA also requires that VLOPs and VLOSEs conduct independent auditing of their compliance with the DSA's obligations, including codes of conduct and crises protocols (European Union, 2022[49]). Moving forward, the development of baselines for comparisons, as well as clarifying distinctions between types of audits (such as algorithmic impact assessments, bias impact assessments, and accurate labelling of algorithmic systems), will be needed to ensure consistency across the industry (Singh and Doty, 2021[50]). Governments could facilitate comparability of platforms' audits and risk mitigation activities by developing specific and quantifiable tests, standards, and processes (Forum on Information and Democracy, 2020[51]).

Beyond the actions and tools, governments must also identify which institutions will enforce regulations. Given the fundamental role information plays in democracy and the potential implications for freedom of expression, ensuring regulatory agencies are independent from the government and from those it regulates can provide greater confidence that decisions are fair and impartial (OECD, 2012[48]). Furthermore, the range of regulatory strategies implicated in reinforcing information integrity across media and communication sectors point to the challenge in identifying the appropriate actor(s) to enforce regulations. The increasing role and impact of digital content means that authorities, including those covering data protection and privacy, competition, media, consumer protection, telecommunications, elections, and others, may all play a role in enforcing regulation in this space.

The European Union DSA, for its part, allows for flexibility on this front. On the one hand, due to the "cross-border nature of the services at stake and the horizontal range of (the DSA's) obligations," the law calls for member states to designate a Digital Services Co-ordinator to "act as the single contact point with regard to all matters related to the application of this Regulation (European Union, 2022[49])." The DSA also notes, however, that Member States may rely on more than one authority, particularly one with specific expertise or enforcement tasks and (such as electronic communications' regulators, media regulators or consumer protection authorities), to support the application of the legislation (European Union, 2022[49]).

4.5. CONSIDERATIONS AND PATH FORWARD

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 evaluation 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.

4.6. METHODOLOGICAL NOTE

The chapter presents an evidence-based analysis of relevant co-ordination mechanism and strategic priorities established at national level to tackle the spread of false and misleading information. This chapter includes data from 24 OECD Member countries obtained from the survey "Institutional architecture and governance practices to strengthen information integrity" designed by the OECD DIS/MIS Resource Hub team (hereafter referred to as "the OECD survey"). The countries participating are Australia, Canada, Chile, Colombia, Costa Rica, Estonia, Finland, France, Greece, Italy, Ireland, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Portugal, Slovak Republic, Spain, Sweden, Switzerland, Türkiye and the United States. Responses were provided by government authorities from April to September 2023. Given the rapid pace of developments in the field of disinformation and information integrity, it is important to note that this chapter reflects the state of affairs in September 2023.

REFERENCES

Amaral, M. et al. (2020), *Principles on effective and innovation-friendly rulemaking in the Fourth Industrial Revolution – Background paper*. [44]

Butcher, P. (2019), "Disinformation and democracy: The home front in the information war", *EPC Discussion Paper*. [7]

European Union (2022), *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*, Publications Office of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?ur. [49]

European Union External Action Service (2023), *1st EEAS Report on Foreign Information Manipulation and Interference Threats*. [1]

Federal Ministry of the Interior and Community (2023), *Measures taken by the Federal Government to fight disinformation*, https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation/measures-taken-by-the-federal-government.html. [16]

Forum on Information & Democracy (n.d.), "International Partnership for Information & Democracy", https://informationdemocracy.org/international-partnership-on-information-democracy/ (accessed on 15 February 2024). [32]

Forum on Information and Democracy (2023), *Pluralism of news and information in curation and indexing algorithms*, https://informationdemocracy.org/wp-content/uploads/2023/08/Report-on-Pluralism-Forum-on-ID.pdf. [31]

Forum on Information and Democracy (2020), *Working Group on Infodemics: Policy Framework*, https://informationdemocracy.org/wp-content/uploads/2020/11/ForumID_Report-on-infodemics_101120.pdf. [51]

Government of Brazil (2023), *Institution of the Committee to Combat Disinformation on the National Program of Immunizations and Public Health Policies*, Presidency of the Presidency of the Republic, https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11753.htm. [18]

Government of Canada (2023), "The Trust Series: Trust and Misinformation in Digital Information Ecosystems (TRN1-E11)", https://catalogue.csps-efpc.gc.ca/product?catalog=TRN1-E11&cm_locale=en. [40]

Government of Canada (2022), "Backgrounder: Government of Canada to fund projects addressing the growing problem of online mis/disinformation", https://www.canada.ca/en/canadian-heritage/news/2022/07/backgroundergovernment-of-canada-to-fund-projects-addressing-the-growing-problem-of-online-misdisinformation.html. [38]

Government of Canada (2022), "Navigating Social Media as a Public Servant (TRN125)", https://catalogue.csps-efpc.gc.ca/product?catalog=TRN125&cm_locale=en. [41]

Government of Canada (n.d.), "Countering Disinformation: A Guidebook for Public Servants", https://www.canada.ca/en/democratic-institutions/services/protecting-democratic-institutions/countering-disinformation-guidebook-public-servants.html (accessed on 15 February 2024). [39]

Government of Ireland (2023), *National Counter Disinformation Strategy Working Group*, https://www.gov.ie/en/publication/04f9e-national-counter-disinformation-strategy-working-group/#. [5]

Government of the Netherlands (2023), *Global Declaration on Information Integrity Online*, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2023/09/20/global-declaration-on-information-integrity-online. [28]

Government of the Netherlands (2023), *Global Declaration on Information Integrity Online*, Ministry of Foreign Affairs, https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2023/09/20/global-declaration-on-information-integrity-online. [29]

Government of the Netherlands (2022), *Government-wide strategy for effectively tackling disinformation*, Ministry of the Interior and Kingdom Relations, https://www.government.nl/documents/parliamentary-documents/2022/12/23/government-wide-strategy-for-effectively-tackling-disinformation. [3]

Government of the Republic of Lithuania (2023), "Lithuania's new crisis management model presented at Baltic States Centres of Government Meeting", The Office of the Government of the Republic of Lithuania, https://lrv.lt/en/news/lithuanias-new-crisis-management-model-presented-at-baltic-states-centres-of-government-meeting/. [10]

Government of the Slovak Republic (2023), *The concept of strategic communication of the Slovak Republic*, https://www.vlada.gov.sk/share/uvsr/koncepcia_strategickej%20komunikacie_sr.pdf?csrt=934388656163986176. [4]

Hybrid CoE (n.d.), "What is Hybrid CoE?", The European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/about-us/ (accessed on 19 October 2023). [24]

IDMO (n.d.), "Uniti contro la disinformazione", Italian Digital Media Observatory, https://www.idmo.it/ (accessed on 10 December 2023). [37]

Instytut Kościuszki (2022), *Report – Resilience to Disinformation*, Instytut Kościuszki, https://ik.org.pl/en/publikacje/4850/. [27]

Jahangir, R. (2023), *Disinformation Landscape in the Netherlands*, EU DisinfoLab, https://www.disinfo.eu/wp-content/uploads/2023/09/20230919_NL_DisinfoFS.pdf. [34]

Jeangène Vilmer, J. (2021), *Effective state practices against disinformation: Four country case studies*. [22]

Kleis Nielsen, R. (2021), *How to respond to disinformation while protecting free speech*. [6]

Latvijas Vēstnesis (2023), "Valsts informatīvās telpas drošības koordinācijas grupas nolikums", Ministru kabineta noteikumi Nr. 236, Rīgā 2023. gada 9. maijā (prot. Nr. 25 28. §), https://likumi.lv/ta/id/341811-valsts-informativas-telpas-drosibas-koordinacijas-grupas-nolikums. [8]

Lewandowsky, S. (2021), "Climate Change Disinformation and How to Combat It", *Annual Review of Public Health*, Vol. 42/1, pp. 1-21, https://doi.org/10.1146/annurev-publhealth-090419-102409. [20]

Ministry of Science, Technology, Knowledge and Innovation (n.d.), "Comisión Asesora contra la Desinformación", https://www.minciencia.gob.cl/areas/comision-contra-la-desinformacion/ (accessed on 15 February 2024). [17]

Ministry of the Interior and Kingdom Relations (2022), *Handreiking omgaan met desinformatie*, Ministry of the Interior and Kingdom Relations, https://www.weerbaarbestuur.nl/sites/default/files/inline-files/BZK%20-%20Handreiking%20omgaan%20met%20desinformatie.pdf. [35]

NATO (2023), "Countering hybrid threats", North Atlantic Treaty Organization, https://www.nato.int/cps/en/natohq/topics_156338.htm. [23]

OECD (2023), *Public Communication Scan of the United Kingdom: Using Public Communication to Strengthen Democracy and Public Trust*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/bc4a57b3-en. [15]

OECD (2022), *Building Trust and Reinforcing Democracy: Preparing the Ground for Government Action*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/76972a4a-en. [47]

OECD (2022), *Recommendation of the Council on International Regulatory Co-operation to Tackle Global Challenges*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0475. [33]

OECD (2021), *OECD Report on Public Communication: The Global Context and the Way Forward*, OECD Publishing, Paris, https://doi.org/10.1787/22f8031c-en. [14]

OECD (2021), *Practical Guidance on Agile Regulatory Governance to Harness Innovation*, OECD. [43]

OECD (2021), "Recommendation of the Council for Agile Regulatory Governance to Harness Innovation", OECD/LEGAL/0464, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464. [45]

OECD (2020), *OECD Public Integrity Handbook*, OECD Publishing, Paris, https://doi.org/10.1787/ac8ed8e8-en. [2]

OECD (2018), *Flexibility and Proportionality in Corporate Governance*, OECD Publishing, Paris, https://doi.org/10.1787/9789264307490-en. [46]

OECD (2018), *OECD Regulatory Policy Outlook 2018*, OECD Publishing, Paris, https://doi.org/10.1787/9789264303072-en. [42]

OECD (2012), "Recommendation of the Council on Regulatory Policy and Governance", *OECD Legal Instruments*, OECD/LEGAL/0390, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0390. [48]

Pamment, J. (2020), *The EU's Role in Fighting Disinformation: Taking Back the Initiative*. [19]

SGDSN (2022), *Service de vigilance et protection contre les ingérences numériques étrangères "VIGINUM"*, Secrétariat général de la défense et de la sécurité nationale, https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques. [11]

Singh, S. and L. Doty (2021), *Cracking Open the Black Box: Promoting Fairness, Accountability, and Transparency Around High-Risk AI*, Open Technology Institute, https://www.newamerica.org/oti/reports/cracking-open-the-black-box/. [50]

State Security Department of Lithuania (2022), "Threat Assessments", https://www.vsd.lt/en/threats/threats-national-security-lithuania/. [9]

Swedish Psychological Defence Agency (2023), *Swedish Psychological Defence Agency website*, Psychological Defence Agency, https://www.mpf.se/en/about-us/ (accessed on 31 August 2023). [12]

TTC (2023), *U.S.-EU Joint Statement of the Trade and Technology Council*, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/31/u-s-eu-joint-statement-of-the-trade-and-technology-council-2/. [30]

U.S. Department of State (2024), "The Framework to Counter Foreign State Information Manipulation", https://www.state.gov/the-framework-to-counter-foreign-state-information-manipulation/. [26]

U.S. Department of State (n.d.), "About Us – Global Engagement Center", https://www.state.gov/about-us-global-engagement-center-2/ (accessed on 31 August 2023). [13]

UK Government Communication Service (2021), *RESIST 2 Counter Disinformation Toolkit*, Government Communication Service, https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/. [36]

UNDP (2021), *Information Asymmetries in the Digital Sexual and Reproductive Health Space*. [21]

UNESCO (2023), *Guidelines for Regulating Digital Platforms: Safeguarding freedom of expression and access to information through a multi-stakeholder approach*, United Nations Educational, Scientific and Cultural Organization, https://unesdoc.unesco.org/ark:/48223/pf0000387339. [25]

NOTES

[1] As part of the survey, respondents were asked: *"To better understand your priorities moving forward, please indicate the areas where your government will seek to improve over the coming 1-2 years"*, one of the suggested priorities was: Develop, update, or increase relevance of guidelines and/or strategic documents.

[2] As part of the survey, respondents were asked: *Is there a national strategic framework or guidance document in force in which the government identifies and describes the main information threats, potential impacts, and response options?*

[3] National Cybersecurity Strategy IV https://hcpn.gouvernement.lu/dam-assets/fr/publications/brochure-livre/strategie-nationale-cybersecurite-4/National-Cybersecurity-Strategy-IV.pdf.

[4] As part of the survey, respondents were asked *"Does a cross-government mechanism (cell, office, unit, etc.) exist to co-ordinate government efforts to identify and/or respond to disinformation?"*.

[5] As part of the survey, respondents were asked: "*To better understand your priorities moving forward, please indicate the areas where your government will seek to improve over the coming 1-2 years*", one of the suggested priorities was: Expanding co-operation with partner countries.

[6] For additional information, see: https://www.oecd.org/stories/dis-misinformation-hub/.

[7] For additional information, see the work of the OECD's Artificial Intelligence Policy Observatory (https://oecd.ai/en/) and the OECD hosting the Secretariat of the 29-member Global Partnership on Artificial Intelligence (GPAI) (https://gpai.ai/).

[8] For additional information, see the work of the OECD Development Assistance Committee's Network on Governance (GovNet): https://www.oecd.org/dac/accountable-effective-institutions/about-govnet.htm.

[9] For additional information, see the Voluntary Transparency Reporting Framework: https://www.oecd.org/digital/vtrf/.

[10] For additional information: https://euvsdisinfo.eu/about/.

[11] For additional information, see: https://www.unesco.org/en/media-information-literacy.

[12] For additional information, see: https://www.undp.org/policy-centre/oslo/information-integrity.

[13] For additional information, see: https://summitfordemocracyresources.eu/about/about-the-summit-for-democracy/.

Facts not Fakes

TACKLING DISINFORMATION, STRENGTHENING INFORMATION INTEGRITY

Rising disinformation has far-reaching consequences in many policy areas ranging from public health to national security. It can cast doubt on factual evidence, jeopardise the implementation of public policies and undermine people's trust in the integrity of democratic institutions. This report explores how to respond to these challenges and reinforce democracy. It presents an analytical framework to guide countries in the design of policies, looking at three complementary dimensions: implementing policies to enhance the transparency, accountability, and plurality of information sources; fostering societal resilience to disinformation; and upgrading governance measures and public institutions to uphold the integrity of the information space.

OECD
Reinforcing
Democracy
Initiative

PRINT ISBN 978-92-64-98010-5
PDF ISBN 978-92-64-37311-2