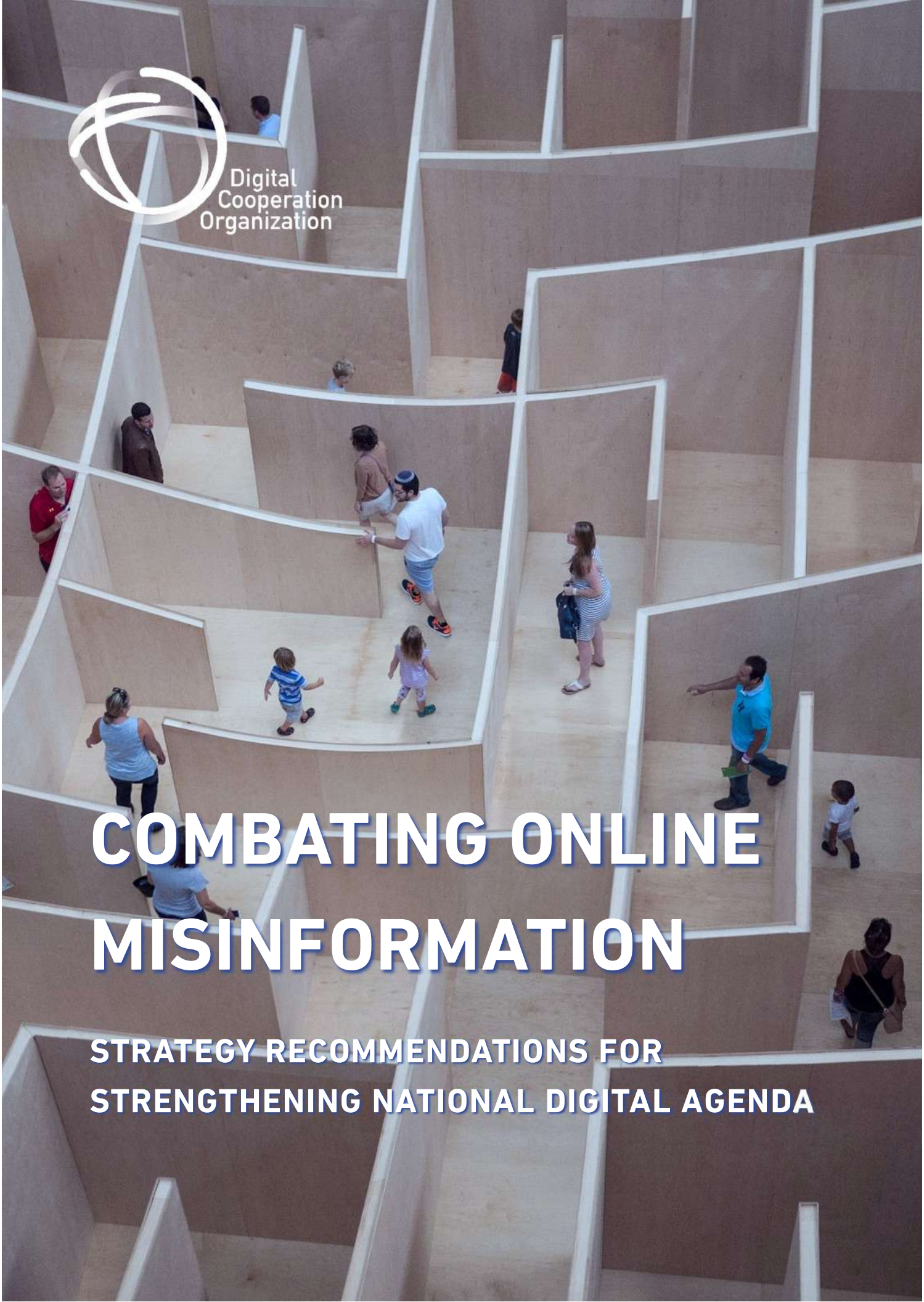


COMBATING ONLINE MISINFORMATION

STRATEGY RECOMMENDATIONS FOR STRENGTHENING NATIONAL DIGITAL AGENDA

TABLE OF CONTENTS

Document Disclaimer

The following legal disclaimer ("Disclaimer") applies to this document ("Document") and by accessing or using the Document, you ("User" or "Reader") acknowledge and agree to be bound by this Disclaimer. If you do not agree to this Disclaimer, please refrain from using the Document.

This Document, prepared by the Digital Cooperation Organization (DCO). While reasonable efforts have been made to ensure accuracy and relevance of the information provided, DCO makes no representation or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability of the information contained in this Document.

The information provided in this Document is intended for general informational purposes only and should not be considered as professional advice. DCO disclaims any liability for any actions taken or not taken based on the information provided in this Document.

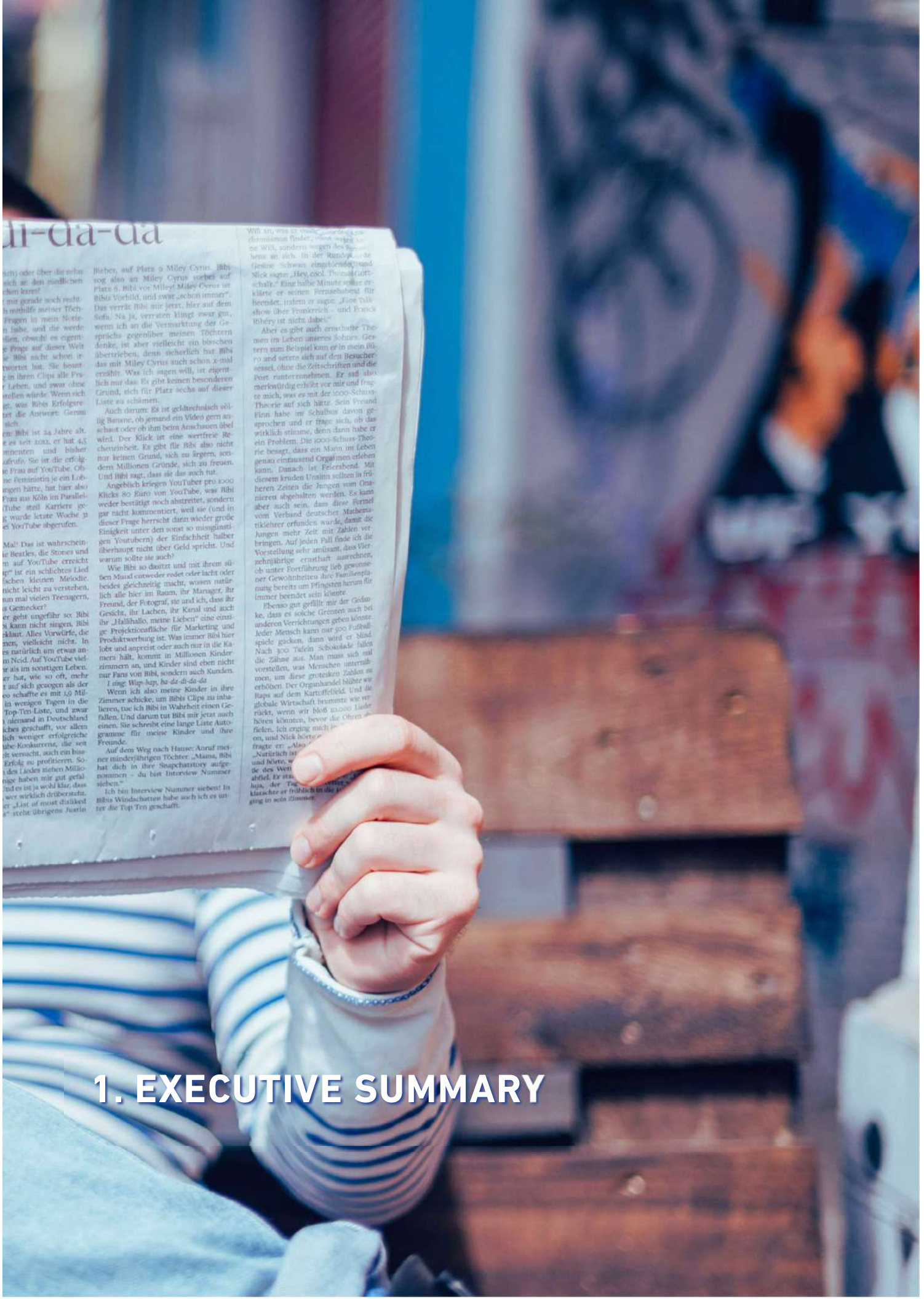
DCO reserves the right to update, modify or remove content from this Document without prior notice. The publication of this Document does not create a consultant-client relationship between DCO and the User.

The designations employed in this Document of the material on any map do not imply the expression of any opinion whatsoever on the part of DCO concerning the legal status of any country, territory, city, or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The use of this Document is solely at the User's own risk. Under no circumstances shall DCO be liable for any loss, damage, including but not limited to, direct or indirect or consequential loss or damage, or any loss whatsoever arising from the use of this Document.

Unless expressly stated otherwise, the findings, interpretations and conclusions expressed in this Document do not necessarily represent the views of the Digital Cooperation Organization. The User shall not reproduce any content of this Document without obtaining DCO's consent or shall provide a reference to DCO's information in all cases.

By accessing and using this Document, the Reader acknowledges and agrees to the terms of this Disclaimer, which is subject to change without notice, and any updates will be effective upon posting.



1. EXECUTIVE SUMMARY

The rapid evolution of the digital landscape has revolutionized information dissemination and consumption, providing unprecedented access to knowledge while simultaneously facilitating the spread of misinformation. The COVID-19 pandemic and the migration crisis among other things have intensified the spread of misinformation, highlighting the urgent need for effective digital strategies to combat false and misleading content that threatens public health, undermines trust in institutions, disrupts social cohesion, jeopardizes democratic processes, and protects the global digital economy from the dangers of misinformation.

This report presents a comprehensive analysis of existing digital strategies, norms, and standards offering recommendations for nations to integrate into their national digital agendas to effectively combat misinformation across various jurisdictions.

International strategies to combat misinformation emphasize collaboration between governments, civil society, media organizations, and the private sector. Organizations like the OECD, the United Nations, and the EU promote media literacy, transparency, and cross-border cooperation to tackle the global nature of misinformation. These strategies prioritize adaptability to new technologies, ethical governance, and public awareness to ensure a coordinated response to the challenges of misinformation.

Legal norms vary across nations, shaping how misinformation is defined, penalized, and who is held accountable. Some countries focus on public safety, while others emphasize digital rights and free speech. Norms behind interventions, such as public awareness campaigns and fact-checking, foster a societal expectation of truth and accuracy, embedding responsibility and integrity in information-sharing practices.

Tools and platforms combat misinformation using clear standards for content moderation, verification, and transparency. These include benchmarks for algorithms, fact-checking systems, and media literacy tools. Social media platforms enforce standards for verifying information, flagging false content, and ensuring transparency in their operations. Together, these tools and platforms uphold accuracy and trust in the digital space.

The report, centered on providing recommendations for the nations, concludes with a call for strengthened cooperation, increased awareness, digital literacy, and continuous evaluation of strategic measures to combat online misinformation, and safeguard the global digital economy from this societal challenge.

2. INTRODUCTION

2.1 Background and context

The digital landscape has transformed the way information is disseminated and consumed, leading to unprecedented access to knowledge and communication. However, this transformation has also given rise to significant challenges, particularly the proliferation of misinformation.

The migration crisis as well as health-related disasters like the COVID-19 pandemic or the monkeypox have exacerbated these challenges, as the urgent need for timely information has often been met with a surge of false and misleading content. This phenomenon has not only threatened public health responses but has also undermined trust in institutions, disrupted social cohesion, and jeopardized democratic processes.

In response to the growing threat of misinformation, nations and international organizations have increasingly recognized the need for comprehensive strategies, norms, and standards to combat this issue.

In response to the growing threat of misinformation, nations and international organizations have increasingly recognized the need for comprehensive strategies, norms, and standards to combat this issue.

A variety of legislative measures, policies, and frameworks have been introduced globally, reflecting diverse approaches to defining, addressing, and penalizing misinformation. These responses have been shaped by the unique socio-political contexts of each jurisdiction, leading to a patchwork of regulations that vary widely in their scope, effectiveness, and enforcement mechanisms.

The urgency of addressing misinformation has prompted a multi-stakeholder approach, involving governments, international and inter-governmental

The Digital Cooperation Organization (DCO) has laid crucial groundwork in combating misinformation, providing a solid foundation upon which this report builds. The DCO's extensive work, exemplified by its key documents "From Social Media to Truth: Countering Misinformation for a Thriving Digital Economy" and "Guidelines for Combatting Online Misinformation in the Era of Digital Economy", contributes significantly to global efforts aimed at addressing the pervasive challenge of misinformation. These documents are essential for

governments, international organizations, businesses, and civil society, as they provide a comprehensive understanding of misinformation's impact on society and the economy. By fostering collaboration and promoting strategic interventions, the DCO's work helps to establish a more informed and resilient global digital environment, guiding stakeholders in safeguarding public trust and ensuring sustainable economic development.

This report seeks to contribute to and expand upon the DCO's framework. While the "Guidelines for Combatting Online Misinformation in the Era of Digital Economy" offer a broad framework for addressing misinformation, and "From Social Media to Truth: Countering Misinformation for a Thriving Digital Economy" outlines the challenges and implications of curbing misinformation on social platforms, this report delves deeper into practical interventions necessary to tackle these issues effectively. It transcends general principles by providing real-world examples – such as case studies of successful misinformation mitigation strategies in various countries – and actionable recommendations.

Moreover, the report discusses and recommends specific legal norms and penalties to emphasize accountability and content integrity. It also details service provider responsibilities, such as mandatory transparency reports and cooperation with fact-checking organizations.

These tangible elements make the strategies immediately implementable, equipping policymakers and stakeholders with concrete tools to respond directly to misinformation crises. The report addresses gaps in existing measures by proposing recommendations tailored for real-world application, ensuring strategies are adaptable to evolving technologies like deepfakes and AI-generated content. By translating high-level discussions into actionable plans, it enhances the earlier documents and facilitates their integration into national and international policy agendas.

This report aims to provide a comprehensive analysis of existing digital strategies, norms, and standards aimed at combating misinformation.

In particular, this report aims to provide a comprehensive analysis of existing digital strategies, norms, and standards aimed at combating misinformation. By reviewing national and international strategies, norms, and standards, this analysis seeks to identify best practices, highlight gaps in current approaches, and offer recommendations for strengthening national digital agendas. The findings will contribute to a deeper understanding of how different jurisdictions are responding to the challenges posed by misinformation and will inform future efforts to create a more resilient and informed society in the digital age.

2.2 Methodology

This report employs a literature review to analyze national and global strategies, norms, and standards countering misinformation. It reviews over 100 national legal norms (see Fig. 1 for the map coverage and Table 1 for the list of countries).

In this analysis, eight key international strategies were reviewed from organizations including the North Atlantic Treaty Organization (NATO), the United Nations (UN), the European Union (EU), the Association of Southeast Asian Nations (ASEAN), the Organisation for Economic Co-operation and Development (OECD), the United Nations Educational, Scientific and Cultural Organization (UNESCO), the World Economic Forum (WEF), and the Council of Europe (CoE). These strategies were evaluated to understand their approaches to misinformation.

We conducted a comprehensive analysis of resources cataloged in the RAND Corporation and the Consortium for Elections and Political Process Strengthening (CEPPS) databases.

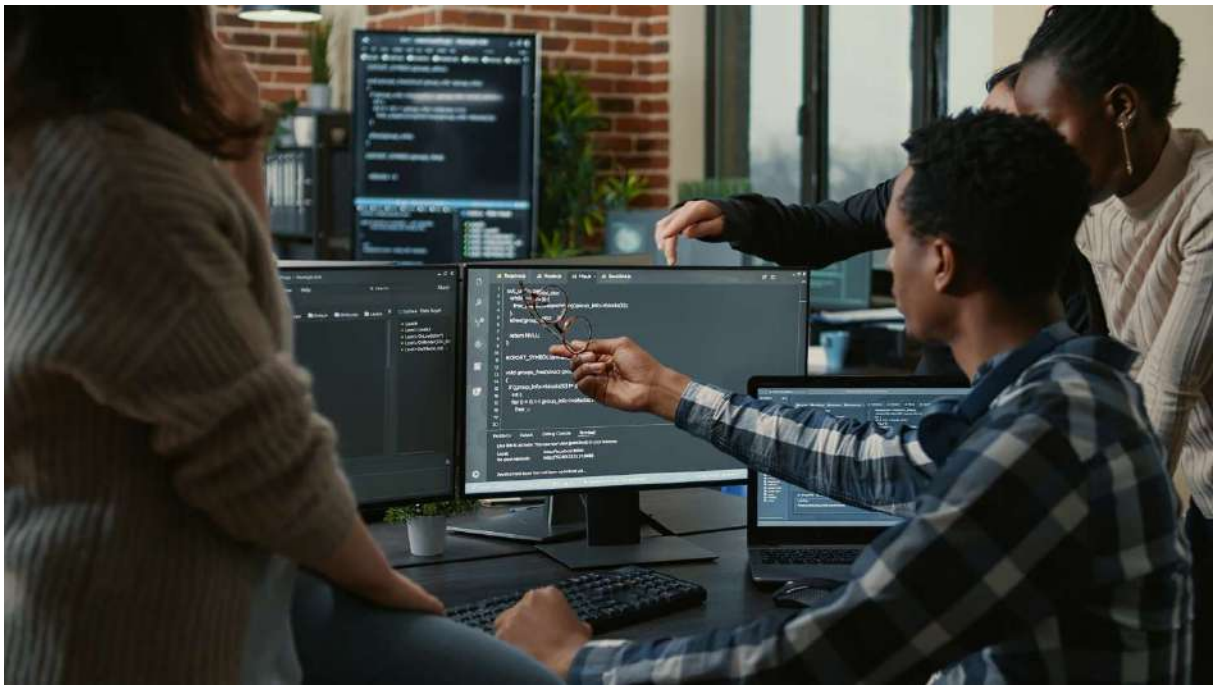
Norms and standards form the foundational backbone of tools and interventions designed to combat misinformation, guiding their development and effectiveness. To investigate this relationship, we conducted a comprehensive analysis of resources cataloged in the RAND Corporation and the Consortium for Elections and Political Process Strengthening (CEPPS) databases. The RAND database, containing over 80 tools, was meticulously examined, and each tool was categorized based on the topics it addresses, such as content moderation, algorithmic transparency, fact-checking, and media literacy initiatives. Similarly, we scrutinized 270 interventions from the CEPPS database, organizing them into thematic clusters including public awareness campaigns, fact-checking endeavors, and policy advocacy efforts. Throughout this analytical process, we focused on assessing the underlying norms and standards that shape these tools and interventions.

Figure 1. Coverage of misinformation laws (Lim & Bradshaw, 2023 + DCO member states that have misinformation legal norms)

Table 1. List of countries with misinformation legal norms (Lim & Bradshaw, 2023 + DCO member states that have misinformation legal norms)

Africa (31)			Asia (19)		Middle East and North Africa (12)
Angola	Ghana	Senegal	Bangladesh	Pakistan	Algeria
Benin	Guinea	Sierra Leone	Cambodia	Philippines	Bahrain
Botswana	Kenya	Somalia	China	Singapore	Egypt
Burkina Faso	Lesotho	South Africa	Kazakhstan	Sri Lanka	Jordan
Cameroon	Madagascar	Sudan	Kyrgyzstan	Taiwan	Kuwait
Chad	Mauritania	Tanzania	Laos	Tajikistan	Morocco
Cote d'Ivoire	Namibia	The Gambia	Malaysia	Thailand	Oman
Djibouti	Niger	Togo	Mongolia	Uzbekistan	Qatar
Eswatini	Nigeria	Uganda		Vietnam	Saudi Arabia
Ethiopia	Rwanda	Zimbabwe	Myanmar		Syria
Gabon			Nepal		Turkey
					United Arab Emirates

Europe (10)		Latin America and the Caribbean (5)	Oceania (3)	Eurasia (2)	North America (2)
Belarus	France	Bolivia	Australia	Azerbaijan	Canada
Bosnia-Herzegovina	Greece	Brazil	Fiji	Russia	United States of America
Cyprus (proposal)	Hungary	Costa Rica	Vanuatu		
Denmark	Malta	Cuba			
	Moldova	Nicaragua			
	Romania				



2.3 Objectives and scope

The primary objective of this report is to provide a thorough analysis of existing digital strategies, norms, and standards aimed at combating misinformation, with the goal of identifying best practices and gaps in current approaches.

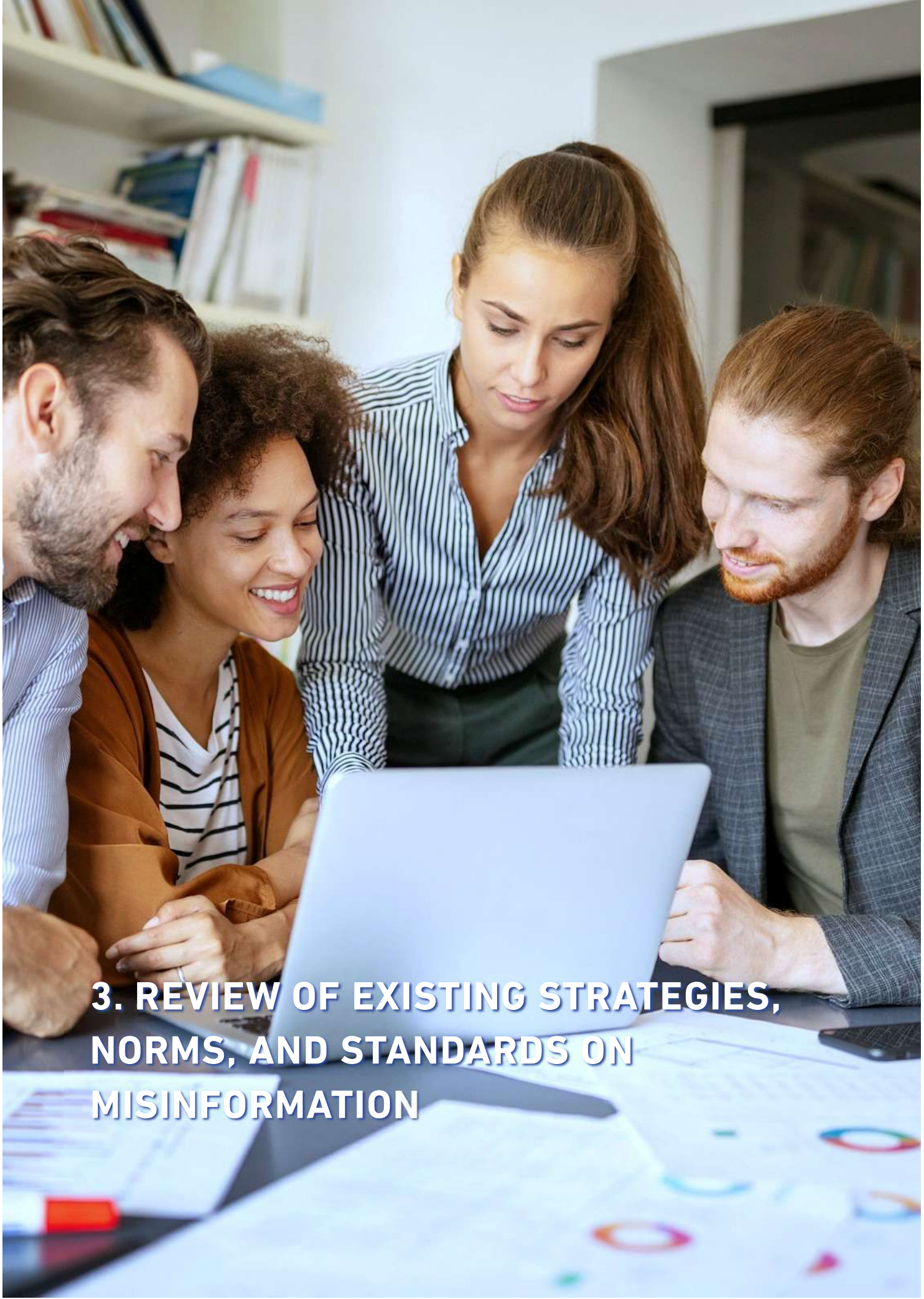
The primary objective is to provide a thorough analysis of existing digital strategies, norms, and standards aimed at combating misinformation, with the goal of identifying best practices and gaps in current approaches.

By examining current national and international strategies, norms, and standards, this analysis seeks to inform policymakers, through strategic recommendations, and other related stakeholders about effective strategic measures to enhance public resilience against misinformation, promote media literacy, and foster a collaborative environment among governments, civil society, and businesses, including technology companies (see Fig. 2) to promote safe, and sustainable digital economy.

Figure 2. Objectives and scope of the analysis

Identify and analyze existing strategies, norms, and standards
• Provide a detailed examination of current national and international strategies, norms and standards aimed at combating misinformation.
Develop recommendations
• Formulate practiced-based digital strategy, norm, and standard recommendations for the nations to integrate into their national digital strategies to combat online misinformation.
Promote informed policy making
• Support policymakers in creating resilient and informed societies by offering evidence-based insights and guidelines to enhance the safe, and sustainable digital economy.

This document is structured as follows. In Section 3, the report provides a thorough review of existing strategies, norms, and standards on misinformation. Section 4 offers recommendations for combating misinformation. Finally, Section 5 concludes the report by summarizing the key insights.



3. REVIEW OF EXISTING STRATEGIES, NORMS, AND STANDARDS ON MISINFORMATION

In addressing complex online misinformation, strategies, norms, and standards form the foundation for effective governance and control.

Strategies refer to the overarching plans and coordinated efforts developed to achieve specific goals. In the context of combating misinformation, strategies provide a structured roadmap for governments, organizations, and platforms to address the spread of false information.

Norms are the accepted behaviors and principles within a society. They can take various forms, including legal norms, which are formalized into laws. Legal norms provide the framework for what is permissible and enforceable by the state. Laws on misinformation define its parameters, identify accountable parties, and outline penalties for violations. Thus, legal norms shape how societies uphold truth and trust in information dissemination.

Standards are measurable benchmarks that establish minimum requirements for compliance, quality, or performance. In the context of misinformation, standards provide clear guidelines for digital platforms, content moderation, and transparency, ensuring a consistent and accountable approach to managing information integrity.

Importantly, strategies, norms, and standards exist both at the national and international levels. Nationally, governments formulate laws and policies specific to their cultural and political environments. Internationally, organizations such as the European Union, NATO, and the United Nations develop broader frameworks that transcend borders, addressing the global nature of misinformation. By harmonizing national and international efforts, a more resilient and informed global digital ecosystem can be cultivated.

3.1 National norms

In this section, we undertake a comprehensive review of national norms, with a particular focus on legal norms embedded in national laws. While laws are formal, enforceable mandates, they also reflect the broader behavioral expectations of a society. By examining these legal norms, we gain insight into how different countries address the challenge of misinformation, defining what constitutes acceptable conduct in the digital information space. This review explores the varying approaches to defining misinformation, the penalties associated with its spread, and the roles of individuals and platforms in maintaining content integrity. Through this analysis, we aim to identify key legal frameworks and norms that shape national responses to misinformation and evaluate their effectiveness in the context of rapid technological advancements and global challenges.

In particular, our comprehensive review of national legal norms identified several key dimensions in which these norms differ, and which are common across most frameworks. While numerous dimensions were initially considered, we have focused on the primary ones that stand out as essential for effective regulation. These include definitions, penalties, responsibility and accountability, adaptation to novel technologies, and timing (see Fig. 3). These dimensions provide the foundation for addressing the challenges posed by misinformation across different jurisdictions.

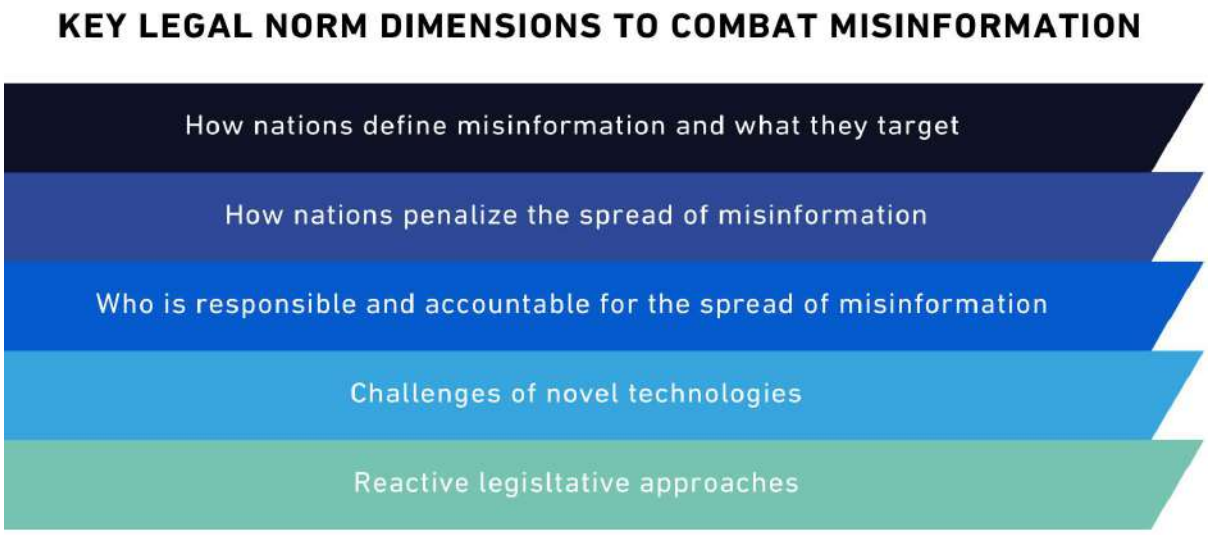
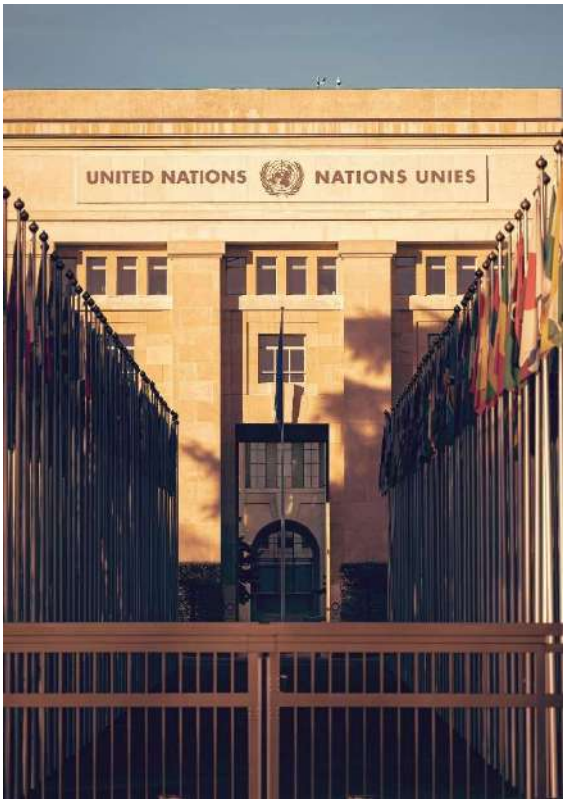


Figure 3. Key legal norm dimensions to combat misinformation

3.1.1 How nations define misinformation and what areas they target

In general, misinformation is defined as false or misleading information that spreads, often unintentionally, and can have harmful effects across various sectors of society. It has many components, and its impact varies depending on the area it affects.



Misinformation related to public order and security involves the dissemination of false information that can incite public unrest, disrupt law enforcement efforts, or create confusion during times of civil disorder, protests, or large-scale public events. It can lead to panic, violence, and strain on public institutions responsible for maintaining peace.

Misinformation on political stability and national security targets the political structures of a nation. It often involves misinformation about government actions, policies, or elections, which can undermine trust in democratic processes, destabilize governments, and compromise national security. This type of misinformation may also be used to spread propaganda or foreign influence operations to weaken a country's internal cohesion.

Health and safety misinformation refers to false claims about medical treatments, health risks, or public health measures. It can lead to harmful behavior, such as ignoring health guidelines during a pandemic or using unproven remedies. This type of misinformation poses a significant risk to individual and public health and can overwhelm health services with misinformation-driven crises.

Misinformation concerning economic stability spreads false information about financial markets, employment data, or economic policies. This can lead to panic in markets, consumer mistrust, and disruptions in economic activities. Misleading reports about economic conditions or regulations can cause significant financial instability and long-term economic damage.

Misinformation related to content integrity and cybersecurity is particularly prevalent due to the ease of sharing information on social media platforms. It includes false narratives, hoaxes, or conspiracy theories that spread rapidly, often exploiting algorithms designed to prioritize sensational or controversial content. This type of misinformation can lead to societal polarization and undermine trust in online platforms as reliable sources of information, posing signifi-

cant challenges to maintaining content integrity and safeguarding digital environments from manipulation.

Reputation and defamation misinformation involves false information that damages the reputation of individuals, organizations, or companies. It can take the form of slander, libel, or false claims about a person's or organization's integrity. This type of misinformation has legal implications, often leading to defamation lawsuits or significant reputational harm.

Misinformation in media and journalism undermines the credibility of legitimate news outlets by spreading false information through news channels, whether intentionally or due to poor fact-checking. This erodes public trust in journalism and can blur the line between verified facts and opinions, further polarizing audiences.

Misinformation in special circumstances and emergencies becomes particularly dangerous during crises, such as natural disasters or terrorist attacks. In these contexts, false information can mislead the public about the scale of the event, available resources, or appropriate responses, delaying necessary action and exacerbating the consequences of the emergency.

Misinformation laws around the world are closely tied to broader social and legal norms that guide societal behavior. These laws not only enforce legal accountability but also reflect underlying norms that prioritize public order, national security, and media integrity. Further categorization and examples of specific laws are outlined in Fig. 4.

Legal norms that promote responsible communication in emergencies are supported by misinformation laws that prevent panic and fear, especially during health crises.

Laws are designed to address various societal concerns, such as protecting public order and security, political stability, health and safety, economic stability, and digital spaces. For instance, legal norms that promote responsible communication in emergencies are supported by misinformation laws that prevent panic and fear, especially during health crises. Similarly, the legal norms of fair elections and free speech are reinforced through laws that safeguard electoral integrity and prevent defamation. Misinformation laws also intersect with norms regulating digital spaces, ensuring that online platforms adhere to standards that prevent the spread of false information. These laws often become more stringent in times of emergency, linking legal norms with heightened responsibilities during crises.

Figure 4. How nations define misinformation and what areas they target

3.1.2 How nations penalize the spread of misinformation

Legal norms often establish the thresholds for defining misinformation offenses and outline appropriate legal responses based on the severity of the harm caused.

Penalties and measures to combat misinformation differ across jurisdictions, with legal norms typically guiding the framework for sanctions. These measures cluster around three main types of penalties: imprisonment, fines, and other regulatory actions. Legal norms often establish the thresholds for defining misinformation offenses and outline appropriate legal responses based on the severity of the harm caused.

Imprisonment penalties vary significantly, from short-term sentences of up to one year for minor offenses, to medium-term sentences of up to ten years for misinformation causing significant public harm, and even long-term sentences of up to fifteen years for severe cases, particularly in wartime or during significant public emergencies. Legal norms in some countries may prioritize imprisonment only for instances

where there is clear evidence of malicious intent or serious societal impact, reflecting a balance between freedom of expression and the protection of public order.

Fines are also tiered, with minor fines addressing smaller infractions, moderate fines for more impactful misinformation dissemination, and severe fines reaching substantial amounts for the most egregious offenses. These fines are often regulated by legal norms that define how fines are calculated, sometimes based on the level of influence a party has in disseminating misinformation or the reach of the false content.

Beyond fines and imprisonment, laws often mandate the removal or blocking of false information, particularly during sensitive periods such as elections or public health crises. Legal norms often dictate that service providers are frequently held accountable, required to monitor and report misinformation actively. Transparency and reporting obligations are enhanced for online platforms under these norms, and civil or administrative penalties, such as license revocations and professional bans, are employed to further deter the spread of false information. Regulatory norms may also introduce periodic audits or compliance reviews for platforms to ensure adherence to policies that combat misinformation. These multi-faceted approaches, grounded in established legal norms, underscore the global recognition of the serious threat posed by misinformation to public order, health, and security. Also see Fig. 5 for details.

Figure 5. How nations penalize the spread of misinformation

Imprisonment	Fines	Other measures
Short-term: • up to one year for spreading misinformation in public meetings, media, etc. • up to three years for spreading misinformation through social media or broadcast media with a large audience. • up to five years for knowingly making false representations to obtain benefits or using them improperly. Medium-term: • up to ten years for disseminating misinformation that causes significant public harm (e.g., during pandemics). Long-term: • up to fifteen years for severe cases where misinformation causes serious public harm (e.g., during war).	Minor: • from small amounts for publishing false information about public health issues up to moderate amounts for false representation and misuse of benefits. Moderate: • for misinformation via large social media or broadcast channels. Severe: • for spreading misinformation that results in substantial public harm or during significant events such as elections.	Content removal and access blocking: • immediate removal or blocking of misinformation upon notification, especially during electoral periods or public health emergencies. Service provider responsibilities: • obligations for social media and other online service providers to monitor, remove, and report false information promptly. Transparency and reporting: • enhanced transparency requirements for online platforms during critical periods to prevent misinformation campaigns. Civil and administrative penalties: • bans on certain professional activities, revocation of licenses, and other administrative actions against responsible entities.

3.1.3 Who is responsible and accountable for the spread of misinformation

The spread of misinformation is addressed differently across various legal frameworks, with accountability assigned to both users who disseminate misinformation and platforms that host content. Legal norms play a critical role in defining the scope of responsibility and penalties for both individuals and platforms, ensuring that sanctions align with national priorities and legal principles.

For example, in Cote d'Ivoire, users who communicate false information through an information system that causes harm or panic are punishable by imprisonment and fines. These penalties are grounded in legal norms that aim to safeguard public order and prevent panic. Similarly, in Uganda, individuals transmitting false information or fraudulent distress signals can face fines and imprisonment, reflecting legal norms that prioritize public safety. In Vanuatu, legal norms hold users spreading false information that harms public order or exposes others to ridicule accountable through imprisonment.

In France, legal norms specific to electoral periods impose penalties on individuals spreading false information to influence elections, with sanctions including imprisonment and fines. In Sudan, publishing false news online that causes panic or undermines the state is punishable by imprisonment, as regulated by legal norms aimed at maintaining national stability.

Various countries also place responsibilities on platforms, based on specific regulatory norms. For example, in Turkey, legal norms mandate social network providers to comply with content removal orders within 24 hours and hold them liable for damages if they fail to act promptly. In Pakistan, legal norms require social media companies to remove unlawful content within 24 hours upon notification and impose penalties for non-compliance. Vietnam enforces legal norms that mandate platforms to implement measures to prevent and remove false information when requested by the authorities.

> In some jurisdictions, both individuals and platforms are held responsible under comprehensive legal frameworks.

In some jurisdictions, both individuals and platforms are held responsible under comprehensive legal frameworks. For example, Singapore's Protection from Online Falsehoods and Manipulation Act allows the government to direct individuals and platforms to correct or remove false information, with non-compliance resulting in fines and imprisonment, as outlined in legal norms designed to ensure information integrity. In the United States, the Countering Foreign Propaganda and Disinformation Act involves coordinated efforts among various agencies and platforms to counter misinformation and support accurate reporting, based on legal norms that emphasize both national security and information accuracy.

3.1.4 Challenges of novel technologies in misinformation control

Mostly, nations do not specifically address adaptation to novel technologies like natural language processing (NLP), artificial intelligence (AI), Generative AI, and deep fakes, which play a significant role in the propagation of misinformation. Legal norms governing these emerging technologies remain underdeveloped in many jurisdictions, creating a regulatory gap. Notably, China has implemented legal frameworks that explicitly target the misuse of AI and related technologies. China's regulations, enforced by the Cyberspace Administration, require the disclosure of AI-generated content, such as deep fakes, to prevent the spread of misleading videos. These norms are among the few that directly address the challenges posed by AI-driven misinformation.

The current legislative landscape reveals a substantial gap in addressing the specific challenges posed by these advanced technologies. There is a pressing need for comprehensive strategic frameworks and legal norms that mandate transparency in the use of AI, ensure accountability, and adapt to rapid technological advancements. Effective management of AI-generated misinformation requires not only national regulation but also international cooperation, public awareness, and education to empower individuals to critically assess the information they encounter. Establishing global legal norms to harmonize efforts across borders could be key in mitigating the risks posed by AI-driven misinformation.

3.1.5 Reactive legislative approaches

Most of the misinformation laws were introduced during or shortly after the onset of the COVID-19 pandemic. These laws are shaped by legal norms that aim to protect public health and maintain social order in times of crisis.

Most of the misinformation laws were introduced during or shortly after the onset of the COVID-19 pandemic. These laws are shaped by legal norms that aim to protect public health and maintain social order in times of crisis.

For example, in 2020, Algeria introduced amendments to the Penal Code to impose penalties for the dissemination of false or slanderous information that could undermine public security or disrupt public order, grounded in legal norms focused on safeguarding national stability. Similarly, Angola amended the Penal Code in 2020 to prohibit the dissemination of false news and propaganda against national defense and armed forces, reflecting legal norms that prioritize national security.

In 2020, Azerbaijan broadened the scope of the Information Law to include users responsible for prohibited content online, including false information related to COVID-19, aligning with legal norms governing online behavior and information dissemination. Bosnia-Herzegovina introduced measures in 2020 against spreading panic and fake news regarding the coronavirus outbreak, supported by legal norms designed to prevent public disorder. Botswana enacted provisions under the Emergency Powers Regulations in 2020, introducing penalties for publishing information intended to deceive about COVID-19, in accordance with legal norms addressing emergency powers and misinformation during health crises.

Cuba introduced a decree in 2020, focusing on the spread of false information in media and online regarding COVID-19, rooted in legal norms aimed at regulating media content and protecting public health. Russia enacted the 2020 COVID-19 Fake News Law, which imposes penalties for disseminating unreliable information about the pandemic, reflecting legal norms designed to control the spread of harmful misinformation during emergencies.

The timing of these legislative actions indicates a reactive approach, primarily responding to the immediate and severe impacts of the COVID-19 pandemic and the associated spread of misinformation. This reactive strategy is characterized by swift legislative changes aimed at controlling the surge of false information that could harm public health efforts, cause panic, and disrupt social order. Legal norms during this period evolved rapidly to address the novel challenges posed by the pandemic and ensure public safety.

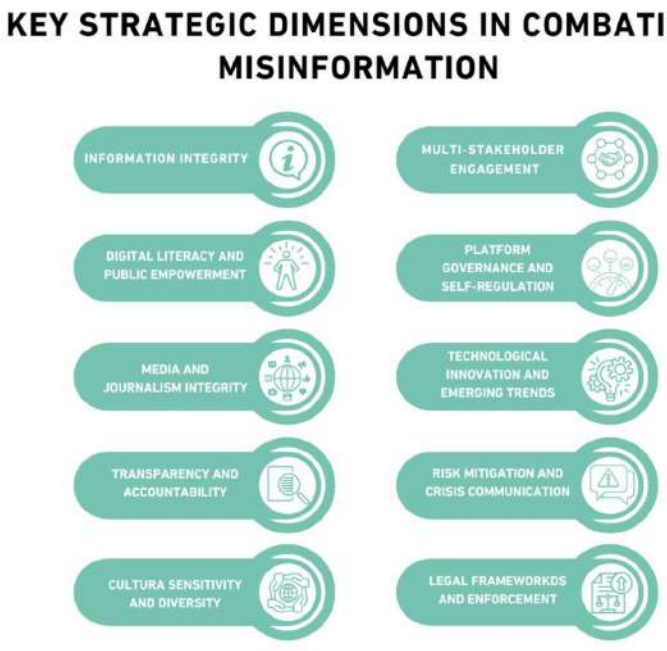


Figure 6. Key strategic dimensions in combatting misinformation

3.2 International strategies

We also reviewed international strategies on combating misinformation. In particular, we analyzed policies by the North Atlantic Treaty Organization (NATO), the United Nations (UN), the Association of Southeast Asian Nations (ASEAN), the Organisation for Economic Co-operation and Development (OECD), the European Union (EU), the United Nations Educational, Scientific and Cultural Organization (UNESCO), the World Economic Forum (WEF), and the Council of Europe (CoE).

By targeting various dimensions such as digital literacy, multi-stakeholder collaboration, information integrity, and platform governance, these international strategies converge on the goal of combating misinformation while adapting their approaches to their respective operational contexts. Below we discuss the main dimensions that we identified in the international strategies (see Fig. 6).

3.2.1 Information integrity

Information integrity refers to the accuracy, consistency, and trustworthiness of information.

Information integrity refers to the accuracy, consistency, and trustworthiness of information.

In an increasingly interconnected world, organizations and institutions at global and regional levels have adopted varying approaches to maintain this integrity, depending on their focus areas and objectives. The core principle across all these bodies is to ensure that the information disseminated and shared is reliable, fostering trust and preventing misinformation, which could disrupt societal stability, security, and development. Global organizations have all emphasized the importance of information integrity but differ in their strategies and focus areas. Their approaches reflect the unique roles they play in promoting global peace, security, development, and cooperation.

NATO and UN both emphasize the integrity of information as a cornerstone in their approach. NATO builds its policy on understanding and engagement, recognizing the need for strategic communication, while the UN promotes multi-stakeholder collaboration to uphold information integrity, especially linked to human rights and peace. On the other hand, OECD and ASEAN prioritize more practical principles around good practices and a comprehensive approach, focusing on transparency and digital literacy, which enhances the credibility of information.

3.2.2 Multi-stakeholder engagement

Multi-stakeholder engagement refers to the involvement of various parties – such as governments, civil society, media, academia, and the private sector – in decision-making processes to ensure diverse perspectives and more holistic solutions. This approach has become particularly important in tackling complex global challenges such as misinformation, governance, and communication strategies in today's interconnected world. Many international and regional organizations advocate for multi-stakeholder engagement, but their approaches differ in scope and focus based on their respective mandates.

NATO and UNESCO both stress the importance of involving multiple stakeholders. NATO focuses on understanding and engagement to counter misinformation, promoting the collaboration of civil society, media, and states. Similarly, UNESCO's multistakeholder approach in platform governance highlights a global effort to address misinformation while maintaining human rights standards. Meanwhile, ASEAN and OECD also take a multi-stakeholder stance, but more focused on regional collaboration and context-specific practices, aiming at creating a coherent public communication strategy at national levels rather than global frameworks.

3.2.3 Digital literacy and public empowerment

Digital literacy, which refers to the ability to navigate, evaluate, and create information using digital technologies, is a critical skill in today's information age. It empowers individuals to make informed decisions, engage responsibly in digital spaces, and identify misinformation.

> Digital literacy empowers individuals to make informed decisions, engage responsibly in digital spaces, and identify misinformation.

Public empowerment through digital literacy plays a pivotal role in the efforts of various global and regional organizations to combat online misinformation and promote trustworthy information ecosystems. Many institutions emphasize the importance of digital literacy and public empowerment, although their approaches vary in scope and focus.

ASEAN focuses significantly on enhancing digital literacy, recognizing it as a foundational element for countering misinfoss-rmation, particularly in the context of fake news. This aligns with WEF's approach, which advocates for public-private cooperation to promote digital media literacy and reduce online harm. UN and EU also address the issue of public empowerment but within a larger framework. The UN Global Principles for Information Integrity include public empowerment as a key dimension, while the EU strengthens this through its Code of Practice, emphasizing transparency and accountability in digital spaces.

3.2.4 Platform governance and self-regulation

Platform governance refers to the policies, rules, and practices that govern how digital platforms operate and manage content, user interactions, and data. As online platforms increasingly shape public discourse and information flows, ensuring responsible governance is essential. Various international and regional organizations advocate for different approaches to platform governance, ranging from self-regulation and co-regulation to public-private cooperation. International organizations have taken notable stances on platform governance and self-regulation, each with unique frameworks designed to balance the interests of platform operators, users, and broader societal goals.

UNESCO and EU both target the dimension of platform governance, advocating for a blend of self-regulation and co-regulation. UNESCO emphasizes diverse participation and safeguarding freedom of expression, while the EU, through its Code of Practice, focuses on strengthening platform governance by aligning with human rights and transparency principles. This contrasts with WEF's approach, which is more centered on public-private cooperation rather than regulatory frameworks. The WEF coalition works towards exchanging best practices, which contributes to digital safety without the explicit regulatory mechanisms.

3.2.5 Media and journalism integrity

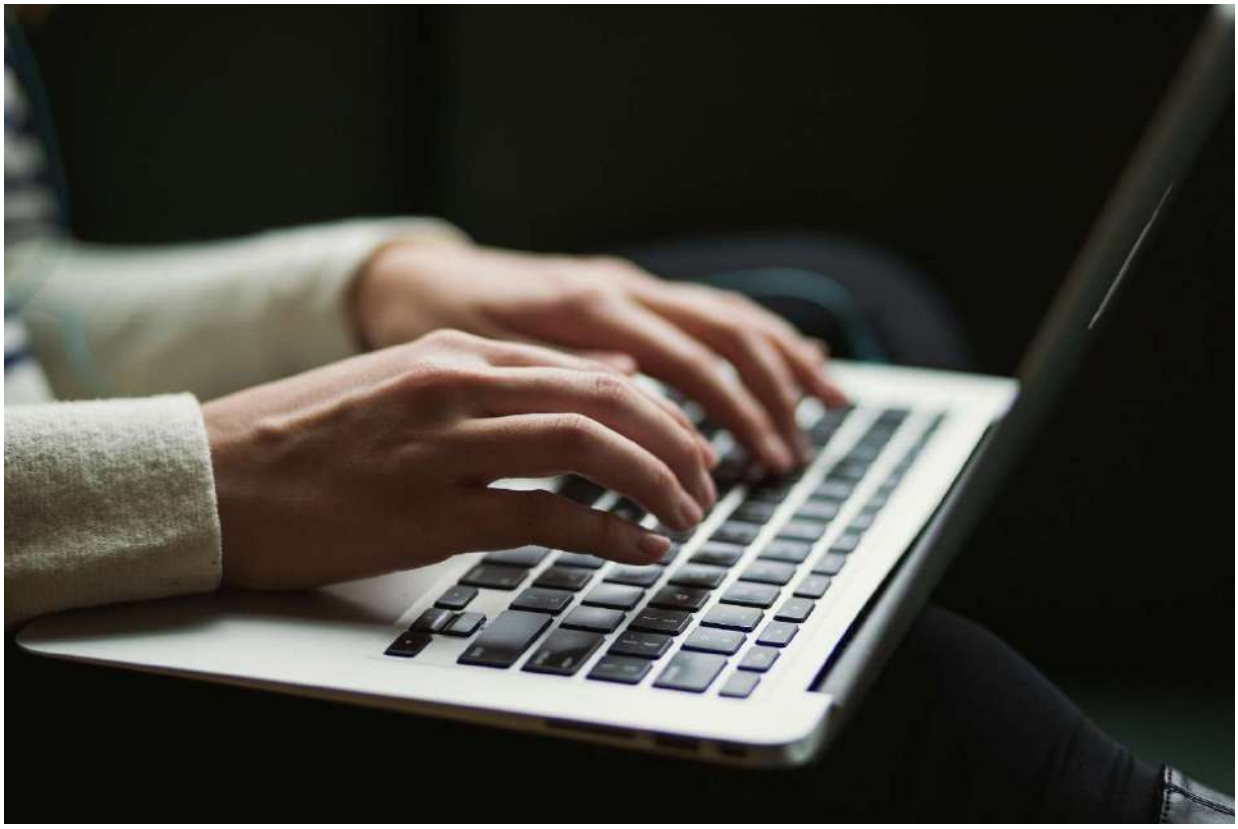
Media and journalism integrity are essential in ensuring that public information is accurate, reliable, and serves the democratic process. In an age where misinformation can undermine public trust and destabilize democratic institutions, maintaining the integrity of media outlets and journalism practices is more critical than ever. International and regional organizations have emphasized different aspects of media integrity to address these challenges.

Council of Europe and UN both highlight the role of media integrity. The Council of Europe focuses on promoting quality journalism as a response to the challenges of misinformation in democratic processes. The UN, through its global principles, also addresses the need for a free and pluralistic media to combat misinformation and protect public trust. OECD and EU similarly address this but through their good practices and codes, focusing on principles that uphold independent media while fostering public accountability.

3.2.6 Technological innovation and emerging threats

The rapid pace of technological innovation, particularly in areas like artificial intelligence, presents both opportunities and challenges in the fight against misinformation. While emerging technologies can be powerful tools in detecting and countering misinformation, they also pose new risks as they can be exploited to spread false information more effectively. International organizations have developed unique strategies to address these challenges, reflecting their broader priorities in digital governance and cybersecurity.

UNESCO and EU both address technological innovation and the challenges posed by emerging technologies, such as artificial intelligence, which can be used both to spread and combat misinformation. UNESCO's guidelines highlight the need to adapt to future challenges, particularly generative AI, in the context of digital platform governance. Similarly, the EU's Code of Practice recognizes the evolving digital ecosystem and the need for new tools and mechanisms to detect and counter misinformation, particularly through algorithms and AI. In contrast, NATO and WEF are more focused on strategic innovations in cybersecurity and digital media monitoring as part of their strategies to combat misinformation, incorporating technologies that enhance digital safety.



3.2.7 Transparency and accountability

Transparency and accountability are essential principles in addressing the spread of misinformation, particularly in digital spaces where information flows rapidly and can easily be manipulated. These principles ensure that information environments are trustworthy, that digital platforms are responsible for the content they host, and that the public can make informed decisions. International organizations place a strong emphasis on these pillars, each contributing to global efforts to combat misinformation through transparent and accountable governance models.

OECD, EU, and UNESCO emphasize transparency and accountability as key pillars for combating misinformation. OECD focuses on creating frameworks for public communication that are transparent and accountable, ensuring that information environments are trustworthy and conducive to public trust. Similarly, the EU's Code of Practice is built on commitments by platforms to ensure transparency in advertising, political communications, and content moderation processes. UNESCO also stresses platform transparency, ensuring that governance models hold digital platforms accountable for misinformation while promoting open access to information.

3.2.8 Risk mitigation and crisis communication

In an era where misinformation can rapidly spread and exacerbate crises, risk mitigation and crisis communication are crucial strategies employed by international organizations to protect public trust, security, and democratic processes. International institutions have developed approaches to address these challenges, focusing on proactive communication, early-warning systems, and safeguarding democratic integrity.

NATO and Council of Europe integrate the concept of risk mitigation into their strategies. NATO emphasizes crisis communication as part of its broader strategic efforts to counter misinformation during conflicts or security crises. The Council of Europe similarly addresses the role of risk communication in democratic settings, focusing on protecting election integrity and democratic discourse from misinformation. OECD and WEF focus on risk management through proactive public communication strategies and the establishment of early-warning systems for harmful online content.

3.2.9 Cultural sensitivity and diversity

Cultural sensitivity and diversity play a crucial role in effectively addressing misinformation in an increasingly interconnected yet culturally diverse world.

Cultural sensitivity and diversity play a crucial role in effectively addressing misinformation in an increasingly interconnected yet culturally diverse world.

Recognizing that different cultural contexts require tailored strategies, international organizations emphasize the importance of incorporating cultural nuances into their efforts to combat misinformation. By promoting cultural expression, inclusive governance, and regional collaboration, these organizations aim to build resilience against misinformation while respecting and leveraging cultural diversity.

UNESCO particularly focuses on cultural diversity as a dimension in addressing misinformation, recognizing that different cultural contexts require tailored approaches. UNESCO's principles encourage fostering cultural expression and maintaining global cooperation to avoid fragmentation of the internet based on cultural differences, while promoting inclusive governance models. ASEAN also addresses this indirectly by promoting regional collaboration and adapting its strategies to the unique sociopolitical landscapes of its member states, focusing on building regional resilience against misinformation.

3.2.10 Legal frameworks and enforcement

The rise of misinformation, particularly in digital spaces, has led various international organizations to develop legal frameworks and enforcement mechanisms to address the issue. The EU and Council of Europe are more aligned in addressing the dimension of legal frameworks to combat misinformation. The EU's Code of Practice and its ongoing legal frameworks for regulating misinformation align with efforts to enforce rules on digital platforms, particularly concerning political ads and misinformation campaigns. Similarly, the Council of Europe supports legal reforms to promote media integrity and democratic protection. UNESCO and OECD, however, focus on guiding principles for governance and communication, often recommending self-regulation or co-regulation instead of stringent laws to ensure adaptability and flexibility in different jurisdictions.

3.3 Strategic interventions and norms to counter misinformation

In the global effort to combat misinformation, a crucial element is the establishment of norms alongside strategic interventions (see Table 2). Various organizations have designed comprehensive approaches to addressing misinformation by combining technical tools, public awareness, and regulatory measures to create a multi-faceted response. As highlighted in the Database of Informational Interventions on the Countering Disinformation, these initiatives span methodologies, regions, and target audiences, reflecting the complexity of the misinformation ecosystem.

Central to combatting misinformation is the work of fact-checking and verification organizations like Trusted Times, AFP Fact Check, and Africa Check. These organizations play a pivotal role not only by verifying the accuracy of information but also by adhering to established norms for responsible journalism and information dissemination. Their efforts reinforce transparency and reliability in information sharing, helping to build trust in media systems globally. This commitment to verification processes aligns with wider efforts to establish fact-checking as a norm, ensuring that information consumed by the public undergoes rigorous scrutiny.

Moreover, awareness campaigns such as Hablatam, #Defendurreality, and #iamhere serve as key interventions in educating the public about the risks of misinformation. These campaigns embed norms of media literacy and critical thinking into educational outreach, encouraging society to adopt more discerning behaviors when interacting with information online. By promoting these skills, these interventions help create a cultural expectation that individuals should critically assess the reliability of their information sources, making society more resilient to misinformation.

Table 2. Mapping of interventions and norms on combatting misinformation

Intervention	Norm
Fact-checking and verification	Verification as a societal norm, building trust in information integrity.
Awareness campaigns	Public expectation of critically assessing information before accepting it as truth.
Content integrity	A consistent global framework for verifying and moderating content across sectors and platforms.
Crowdsourcing	A culture where individuals actively contribute to maintaining information accuracy and debunking falsehoods.
Policy advocacy	Formalized legal structures holding individuals and organizations accountable for spreading misinformation.
Research-based	Evidence-based decision-making as a central principle in addressing misinformation globally.

One of the most vital developments in this space is the formalization of norms for identifying and combating misinformation. Initiatives such as the Certified Content Coalition and A Guide to Anti-Misinformation Actions are actively working to establish guidelines and best practices for content integrity. These guidelines are intended not just for fact-checkers but also for media outlets, technology companies, and content creators. Their promotion should ensure a consistent approach to countering misinformation across sectors. The guidelines help in shaping global content policies and promote a framework that regulates how information is verified, flagged, and removed. This aligns with global policy efforts to establish a regulatory infrastructure that ensures information integrity is consistently prioritized across platforms and countries.

The role of crowdsourcing in combating misinformation also contributes to the development of community-based norms. Platforms that facilitate public participation in reporting and debunking false information help cultivate a communal norm of vigilance. These efforts embed collective responsibility in identifying and addressing false information. By engaging the public directly, crowdsourcing contributes to establishing societal norms around the importance of truth and the unacceptability of misinformation, fostering a culture where information accuracy is a shared priority.

Policy advocacy further anchors the fight against misinformation in formal norms. Initiatives such as the Disinfo Defense League Policy Platform work directly with legislators and international regulatory bodies to embed efforts to combat misinformation into legal frameworks. By pushing for the adoption of policies and regulations, these organizations help to institutionalize the fight against misinformation, ensuring that norms are enforced through legal mechanisms. This creates a structured environment where misinformation is addressed not only by voluntary efforts but also through binding regulations that hold individuals and organizations accountable for spreading falsehoods.

Lastly, research-based interventions promote evidence-based approaches to setting norms and policies that are more effective

in addressing specific aspects of misinformation. Studies like A Field Guide to Fake News enable researchers to identify the underlying dynamics of misinformation, offering insights that inform policy development, content moderation practices, and educational standards. Research also contributes to the global harmonization of efforts to combat misinformation, ensuring that strategies are based on a thorough understanding of the problem and can be scaled across different regions and contexts.

3.4 Standards that help combat misinformation

Combating misinformation effectively necessitates not only the deployment of sophisticated technological tools but also the establishment and adherence to comprehensive standards. Standards provide a unified framework that ensures consistency, reliability, and accountability across various strategies aimed at mitigating the spread of false information. They facilitate collaboration among stakeholders, enhance the interoperability of tools, and reinforce public trust in the measures implemented to safeguard information integrity.

Standards provide a unified framework that ensures consistency, reliability, and accountability across various strategies aimed at mitigating the spread of false information.

To address misinformation comprehensively, standards encompass multiple categories, including algorithmic standards for detection and tracking, verification standards for fact-checking, educational standards for media literacy, credibility scoring criteria, and user-guided standards for content filtering. Additionally, international common standards extend beyond tool-specific guidelines to include broader perspectives such as educational initiatives to improve literacy and mandates for social media firms to report and manage misinformation on their platforms. These diverse standards collectively form a robust defense against the multifaceted challenges posed by misinformation.

The development of technological tools to combat misinformation is not only about strategy but also involves the establishment of operational standards that guide how these tools function and interact with users (see Table 3). The review of 82 tools provides a multifaceted landscape. Detection and tracking tools, such as Bot Sentinel and Botometer, operate based on algorithmic standards that ensure consistency in identifying bots and malicious activity. These tools rely on standardized methodologies for detecting coordinated misinformation campaigns, providing users and platforms with a reliable means to track misinformation. The development and refinement of such standards ensure these tools can be widely applied across different platforms, creating a unified approach to recognizing and mitigating misinformation threats.

Table 3. Mapping of tools on standards on combatting misinformation

Tool	Operational standard
Detection and tracking	Algorithmic standards for detecting bots, malicious activity, and coordinated misinformation campaigns.
Fact-checking and verification	Verification standards ensuring credibility and accuracy in assessing claims.
Media literacy and education	Educational standards promoting critical thinking and media literacy.
Credibility scoring	Objective criteria for assessing trustworthiness, such as transparency, source quality, and evidence strength.
Browser extensions and apps	User-guided standards for filtering and flagging misinformation.

Fact-checking and verification tools, such as Factcheck.org, PolitiFact, and Snopes, adhere to established verification standards to provide accurate and trustworthy information. These tools have formalized processes for assessing the credibility of claims, ensuring that each fact-checked statement meets rigorous guidelines for accuracy. The adoption of these standards across fact-checking platforms contributes to creating global benchmarks for content verification, reinforcing public trust in the information provided by these platforms.

Media literacy and education tools, such as Checkology and IREX's Learn to Discern, contribute to the establishment of educational standards in misinformation awareness. These tools promote critical thinking skills and media literacy, which are increasingly recognized as essential competencies for the digital age. By embedding these skills into education systems and public awareness campaigns, these tools help to normalize critical engagement with information, creating societal expectations around the need for verification and discernment when consuming media.

Credibility scoring tools, like The Factual, provide a standardized way of assessing the trustworthiness of information sources. These tools assign credibility scores based on objective criteria, such as author transparency, source quality, and evidence strength. By applying these scoring systems consistently, credibility tools help users make informed decisions about the reliability of their information sources, contributing to the development of standards for media trustworthiness.

Finally, browser extensions and apps, such as Adblock Plus and KnowNews, incorporate user-guided standards for filtering and flagging misinformation. These tools give users control over the type of content they encounter, setting a standard for how online environments should protect individuals from harmful or misleading information. By integrating filtering capabilities directly into the user experience, these tools normalize proactive engagement with content accuracy, making it an expected part of internet browsing behavior.

4. RECOMMENDATIONS FOR COMBATING MISINFORMATION

To provide a comprehensive and forward-looking approach to combating misinformation, this section outlines strategies, norms, and standards based on the findings from Section 3. These recommendations aim to address the gaps identified in national and international frameworks.

Each recommendation highlights **why** it is important (?), explaining the significance of addressing misinformation, **what** to improve (!), identifying gaps or areas needing enhancement based on current findings, and **how** to implement (➔), providing actionable steps to integrate the solution effectively into national strategies.

4.1 Recommended strategies

To effectively combat misinformation, countries should adopt forward-thinking and adaptable strategies that go beyond reactive measures. These strategy recommendations (see Fig. 7) aim to close existing gaps by enhancing proactive frameworks, expanding definitions, and fostering collaboration across sectors and borders. By addressing the evolving challenges posed by novel technologies and high-stakes periods, these strategies will equip nations with the tools to counter misinformation and ensure a more resilient information ecosystem.

Figure 7. Recommended strategies to combat misinformation

a. Clarify and expand definitions of misinformation and target areas

Recommendation: Clarify and expand definitions of misinformation and target areas	One of the major gaps identified is the inconsistent definitions of misinformation across national frameworks. Countries need to adopt digital strategies that clarify and expand these definitions.		
	Why (?)	**What (!)**	**How (➔)**
	Clearly defined terms help legal and regulatory frameworks address misinformation comprehensively, especially as technology evolves.	Incorporate misinformation related to novel technologies like deepfakes and AI-generated content.	Work with legal, technological, and policy experts to craft updated definitions that reflect current and future misinformation forms, establishing mechanisms for periodic review.

To effectively combat misinformation, countries should standardize and broaden misinformation definitions within national frameworks to include emerging forms such as deepfakes and AI-generated content (see 3.1.1 for misinformation definitions and target areas). Clear and comprehensive misinformation definitions ensure that legal and regulatory measures can accurately identify and address various misinformation tactics as technology evolves.

For example, consider the issue of deepfake videos being used to spread false information about political figures. Existing national frameworks with limited definitions of misinformation might not explicitly cover such content, making it challenging to take legal action against its creators or distributors. By clarifying and expanding definitions to include deepfakes and similar technologies, the framework now recognizes these as legitimate forms of misinformation.

b. Adopt proactive approaches to timing and technology

Recommendation: Adopt proactive approaches to timing and technology	Many countries responded reactively to misinformation, particularly during crises like the COVID-19 pandemic. Stakeholders, particularly policymakers, should develop proactive digital strategies to address misinformation before it escalates during sensitive periods such as elections, health emergencies, or national security crises.		
	Why (?)	**What (!)**	**How (➔)**
	Proactive measures prevent crises from escalating due to the spread of misinformation.	Introduce anticipatory measures and frameworks designed to be activated during specific crises.	Establish early-warning systems leveraging AI and social media monitoring tools to detect trends in misinformation and deploy countermeasures in real time.

To effectively manage misinformation, countries should develop proactive digital strategies that anticipate and address misinformation before it escalates during critical periods such as elections, health emergencies, or national security crises. Implementing anticipatory measures and leveraging advanced technologies ensures timely intervention and minimizes the impact of false information.

To effectively manage misinformation, countries should develop proactive digital strategies that anticipate and address misinformation before it escalates during critical periods such as elections, health emergencies, or national security crises.

For example, during the COVID-19 pandemic, misinformation about vaccines and treatments spread rapidly on social media platforms, leading to public confusion and hesitancy. By adopting a proactive approach, policymakers could have established early-warning systems using AI and social media monitoring tools to identify and track misinformation trends in real time. With these systems in place, authorities could have deployed targeted countermeasures, such as issuing accurate information campaigns and correcting false claims promptly, thereby reducing the spread and impact of harmful misinformation before it became widespread.

c. Enhance cross-border cooperation

Recommendation: Enhance cross-border cooperation between nations	Misinformation is often transnational, requiring countries to cooperate in combating cross-border campaigns. A strategy of international collaboration should be formalized to prevent and mitigate the spread of misinformation across jurisdictions.		
	Why (?)	**What (!)**	**How (➔)**
	Cross-border misinformation campaigns undermine national security and public trust. No country can combat this issue alone.	Establish regular information-sharing agreements and joint action protocols with neighboring countries and international bodies.	Leverage platforms like the UN, NATO, and regional organizations (e.g., DCO, EU, ASEAN) to create shared intelligence systems, cross-border fact-checking networks, and joint task forces.

Misinformation often transcends national boundaries, making it essential for countries to collaborate in combating cross-border misinformation campaigns. Formalizing international collaboration strategies helps prevent and mitigate the spread of misinformation across different jurisdictions, thereby strengthening global efforts to maintain public trust and national security.

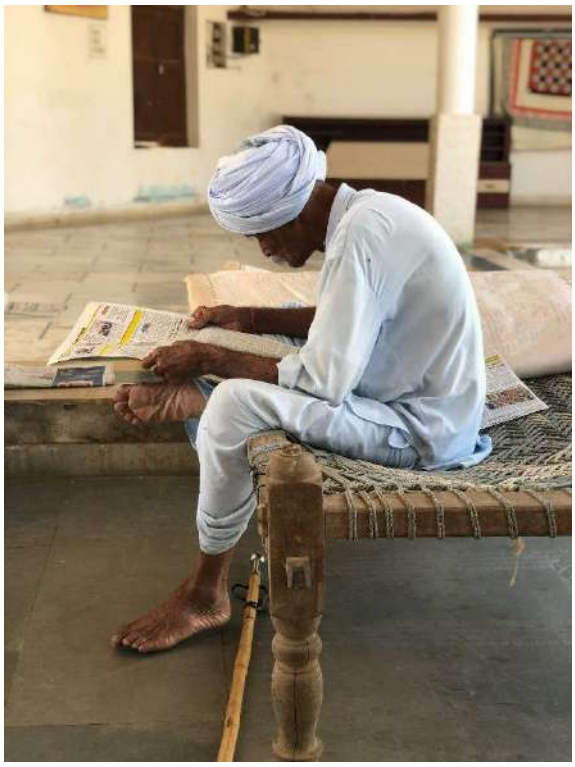
For example, a coordinated misinformation campaign is launched from a foreign country with the intent to influence the outcome of national elections in Country Y by spreading false information about candidates on social media. Under a framework of enhanced cross-border cooperation, Country Y collaborates with its allies through platforms like the EU and NATO to share intelligence and best practices. They establish joint fact-checking networks and real-time information-sharing agreements, enabling swift identification and response to the misinformation campaign. Together, they deploy synchronized countermeasures, such as debunking false claims and educating the public, effectively curbing the campaign's impact and safeguarding the electoral process.

d. Engage in public awareness campaigns focused on vulnerable groups

Recommendation: Engage in public awareness campaigns focused on vulnerable groups	Certain groups, including the elderly, youth, and those in isolated communities, are particularly vulnerable to misinformation. Targeted public awareness campaigns should be part of national strategies, focusing on educating these groups about how to spot and report misinformation.		
	Why (?)	**What (!)**	**How (➔)**
	Tailored campaigns increase the likelihood that vulnerable populations will receive and internalize critical information, reducing their susceptibility to misinformation.	Currently, strategies acknowledge public education but there is no emphasis on specific outreach to vulnerable groups.	Governments can partner with civil society organizations, schools, and local leaders to develop and disseminate culturally sensitive and accessible materials through various media, including social media, radio, and community workshops.

To effectively reduce the impact of misinformation, national digital strategies should include targeted public awareness campaigns tailored to vulnerable populations such as the elderly, youth, and individuals in isolated communities. These campaigns should educate these groups on identifying and reporting misinformation through accessible and culturally sensitive materials distributed via multiple media channels.

For example, during a public health emergency, the government identifies that elderly individuals living in remote areas are particularly susceptible to misinformation about available treatments and preventive measures. To address this, the government collaborates with local community organizations and healthcare providers to develop easy-to-understand pamphlets and radio programs that explain how to recognize false information and where to find trustworthy sources. Additionally, community workshops are held in senior centers where facilitators demonstrate practical steps for verifying information online and encourage attendees to report any suspicious content they encounter. This targeted approach ensures that vulnerable groups receive the necessary tools and knowledge to combat misinformation effectively.



4.2 Recommended norms

Establishing strong norms is essential for creating a societal foundation that supports the fight against misinformation.

Establishing strong norms is essential for creating a societal foundation that supports the fight against misinformation. These norms (see Fig. 8) foster shared accountability, promote ethical behavior in media and digital spaces, and emphasize the importance of public education and collaboration. The following recommendations are designed to guide nations in shaping a culture where transparency, responsibility, and cooperation are prioritized, ensuring that both individuals and organizations contribute to maintaining the integrity of information. By embedding these norms into the fabric of society, countries can build long-term resilience against the spread of false and misleading content.

Figure 8. Recommended norms for combatting misinformation

a. Promote accountability for both platforms and individuals

Recommendation: Promote accountability for both social media and digital platforms and individuals	The limited shared accountability is one of the identified gaps. Norms should ensure shared responsibility between individuals who spread misinformation and platforms that host and amplify it.		
	Why (?)	**What (!)**	**How (➔)**
	Both individuals and platform owners play roles in the spread of misinformation, and holding both accountable ensures a balanced and fair approach.	Instances of shared responsibility are uncommon.	Encourage platforms to take responsibility for content moderation while promoting user education campaigns that teach individuals about the legal and ethical implications of sharing misinformation.

To effectively combat misinformation, it is crucial to establish shared accountability between individuals who spread misinformation and the platforms that host and amplify it. Ensuring

that both parties are responsible creates a balanced and fair approach to reducing the dissemination of misleading content.

For example, when a user on a popular social media or digital platform repeatedly shares false claims about a public health issue, the platform takes action by removing the misleading posts and issuing warnings to the user. Concurrently, the platform launches educational campaigns to inform all users about the legal and ethical consequences of spreading misinformation. This dual approach holds both the individual and the platform accountable, thereby discouraging the spread of false information and promoting a more responsible online environment.

b. Incorporate public education and digital literacy as core values

Recommendation: Incorporate public education and digital literacy as core values	A more robust norm is needed where digital and media literacy are ingrained as a societal responsibility and an essential part of civic education.		
	Why (?)	**What (!)**	**How (➔)**
	An informed public is the best defense against misinformation, as individuals become critical consumers of information.	Expand the digital literacy focus beyond schools to include the wider population, especially underserved groups.	Incorporate digital literacy into national education curricula at all levels, and partner with media organizations and NGOs to roll out public campaigns promoting these values.

To effectively combat misinformation, it is essential to embed digital and media literacy into societal and civic education. This means expanding digital literacy initiatives beyond schools to reach the entire population, with particular attention to underserved groups. By making digital literacy a fundamental aspect of national education curricula and partnering with media organizations and NGOs, societies can empower individuals to critically evaluate information and become responsible consumers and sharers of content.

For example, a country integrates digital literacy into its national education system, starting from primary schools through to higher education. Alongside formal education, the government collaborates with media organizations and NGOs to launch nationwide public awareness campaigns. These campaigns include workshops, online resources, and community seminars aimed at teaching adults in rural and underserved areas how to identify fake news, verify sources, and understand the implications of sharing misinformation. As a result, the general population becomes more skilled at discerning credible information, significantly reducing the spread and impact of misinformation across all segments of society.

c. Foster international collaboration and multi-stakeholder engagement

Recommendation: Foster international collaboration and multi-stakeholder engagement	Norms should encourage international cooperation and multi-stakeholder engagement, which are critical for addressing the global nature of misinformation.		
	Why (?)	**What (!)**	**How (➔)**
	Misinformation often spreads across borders, and cooperation enhances the effectiveness of countermeasures.	Increase the scope and frequency of collaborative efforts between governments, tech companies, civil society organizations, and international bodies.	Set up regular forums for stakeholder collaboration, focusing on cross-border data sharing, joint campaigns, and shared strategies to counter misinformation.

Addressing misinformation effectively requires international cooperation and the involvement of various stakeholders, including governments, private sector companies, civil society organizations, and international institutions. By working together across borders and sectors, countries can enhance the effectiveness of their countermeasures, share valuable intelligence, and develop unified strategies to combat the global spread of misinformation.

For example, several countries facing a coordinated misinformation campaign targeting election processes decide to collaborate through a regional alliance under the European Union. They have regular virtual meetings and create a collaborative intelligence platform where they can quickly exchange information about emerging misinformation trends and sources. Additionally, they partner with major social media companies to implement joint fact-checking initiatives and develop standardized protocols for content moderation. Civil society organizations contribute by organizing public awareness campaigns across multiple countries, educating

citizens on how to recognize and report misinformation. This multi-stakeholder approach ensures a comprehensive and unified response, significantly reducing the impact of the misinformation campaign on the electoral process.

d. Promote transparency in platform operations

Recommendation: Promote transparency in platform operations	Norms should emphasize platform transparency, ensuring that platforms are open about their content moderation practices, algorithmic decisions, and actions taken to counter misinformation.		
	Why (?)	**What (!)**	**How (➔)**
	Transparency builds public trust and ensures platforms are held accountable for their role in amplifying misinformation.	Platforms are not consistently transparent about how they handle misinformation.	Platforms should be required to publish regular transparency reports, including details on misinformation removal, appeals, and algorithmic changes.

To build public trust and ensure accountability, digital platforms should be required to be open about their content moderation practices, algorithmic decisions, and actions taken to counter misinformation. Transparency allows users and regulators to understand how information is managed and ensures that platforms are held responsible for mitigating the spread of false information.

For example, a major social media or digital platform implements a holistic policy requiring the publication of quarterly transparency reports. These reports include data on the number of misinformation posts removed, the criteria used for content moderation, details about algorithm changes that affect content visibility, and information on user appeals processes. By making these reports publicly accessible, the proposed framework enables independent analysts and the general public to assess its efforts in combating misinformation. This openness not only enhances trust among users but also allows for external accountability, ensuring that the platform continuously improves its strategies to address the spread of false information.

4.3 Recommended standards

Implementing clear and enforceable standards is crucial for ensuring consistency, accountability, and fairness in combatting misinformation. These standards (see Fig. 9) provide the legal and operational framework that governs actions related to content moderation, platform accountability, and the responsible use of emerging technologies. The following recommendations aim to establish measurable benchmarks that countries can adopt to strengthen their governance framework and policy environment. By setting these standards, nations can ensure that their efforts to combat misinformation are both transparent and effective, providing a solid foundation for safeguarding public trust and maintaining the integrity of the digital space.

Figure 9. Recommended standards on combatting misinformation

a. Develop clear penalties

Recommendation: Establish explicit penalties for the spread of misinformation	There is a variety of penalties that countries have implemented, but the approaches are inconsistent. Clear, graduated legal standards should be developed, distinguishing between low-level offenses and severe cases of misinformation, such as election interference or public safety threats.		
	Why (?)	**What (!)**	**How (➔)**
	Proportional penalties ensure fairness and act as a deterrent without stifling legitimate free speech.	Penalties lack proportional frameworks for different levels of misinformation.	Governments should develop tiered penalty structures, ranging from fines and community service for minor infractions to imprisonment and steep fines for severe cases.

To ensure fairness and effectiveness in combating misinformation, governments should establish clear and graduated legal penalties. This approach distinguishes between minor offenses and severe cases, such as election interference or threats to public safety, thereby acting as a deterrent while protecting legitimate free speech.

Governments should distinguish between minor offenses and severe cases, such as election interference or threats to public safety, thereby acting as a deterrent while protecting legitimate free speech.

For example, a government enacts a law that categorizes misinformation offenses into different levels. For minor cases, such as sharing unverified rumors on social media, individuals may receive fines or be required to attend educational workshops on media literacy. In more serious instances, like creating and distributing misinformation that influences election outcomes or endangers public health, the penalties escalate to substantial fines and potential imprisonment. If someone is found guilty of spreading false information about election fraud to manipulate voting behavior, they could face significant legal consequences, including hefty fines and a prison sentence. This tiered penalty structure ensures that responses are proportionate to the severity of the misinformation, promoting accountability without unnecessarily restricting free expression.

b. Require platforms to uphold accountability and implement reporting standards

Recommendation: Require platforms to uphold accountability and implement reporting standards	Countries should implement legal standards requiring social media platforms and tech companies to be more accountable in managing and moderating content. Platforms should be held to clear reporting standards on how they handle misinformation.		
	Why (?)	**What (!)**	**How (➔)**
	Holding platforms accountable ensures that misinformation is addressed effectively, and regular reporting provides transparency.	Many frameworks do not sufficiently address platform responsibility.	Require platforms to publish quarterly or annual transparency reports detailing their moderation processes, content removals, appeals, and how their algorithms prioritize content.

To effectively combat misinformation, countries should establish legal requirements that hold social media platforms and tech companies accountable for managing and moderating content. By enforcing clear reporting standards, governments can ensure that platforms transparently address misinformation and continuously improve their moderation practices.

For example, a government passes legislation requiring all major social media platforms to submit detailed transparency reports every quarter. These reports must include the number of misinformation posts removed, the criteria used for content moderation, the outcomes of user appeals, and insights into how their algorithms prioritize or demote certain content. When a platform detects a surge in misinformation about a public health crisis, the transparency report will document the actions taken to remove misleading posts, the rationale behind algorithm adjustments to reduce the visibility of such content, and the effectiveness of these measures based on user feedback and misinformation trends. This mandated accountability

ensures that platforms remain diligent in their efforts to curb misinformation and allows the public and regulators to monitor and assess their performance consistently.

c. Set standards for AI and deepfake disclosures

Recommendation: Set standards for AI and deepfake disclosures	There is a gap in addressing the challenges posed by AI-generated content and deepfakes. Countries should implement standards that require clear labeling and disclosure when content has been altered or generated by AI technologies.		
	Why (?)	**What (!)**	**How (➔)**
	Malicious actors can use AI to deceive the public. Standards ensure that the public can distinguish between authentic and fabricated content.	There are limited efforts to address AI-generated misinformation, which need expansion.	Legislate that platforms and content creators must disclose when videos or images are AI-generated, with penalties for failing to comply.

To address the growing challenges posed by AI-generated content and deepfakes, countries should implement clear standards that require the labeling and disclosure of altered or AI-generated media. These standards help the public easily identify authentic content and reduce the potential for deception by malicious actors using advanced technologies.

For example, a country enacts legislation that mandates all social media platforms and content creators to clearly label any video or image that has been altered or generated using AI technologies. For instance, a deepfake video depicting a public figure making false statements must include a visible disclaimer such as “This content has been artificially generated or altered”. Failure to comply with these standards results in penalties, including fines and restrictions on platform operations. As a result, users can quickly recognize and question the authenticity of suspicious content, thereby minimizing the spread and impact of AI-driven misinformation.

d. Establish crisis-specific standards

Recommendation: Establish crisis-specific standards	Most misinformation laws were enacted reactively during crises like the COVID-19 pandemic. Countries should establish crisis-specific standards that automatically trigger during emergencies, such as heightened penalties or faster misinformation takedown protocols.		
	Why (?)	**What (!)**	**How (➔)**
	Misinformation is particularly harmful during crises, as it can cause panic or undermine public trust in vital institutions.	Pre-established crisis protocols can mitigate the spread of misinformation before it causes harm.	Governments should create legal frameworks that go into effect during declared crises (pandemics, elections, natural disasters), enabling rapid-response teams and stricter penalties for misinformation related to these events.

To effectively manage misinformation during critical times, countries should develop crisis-

specific standards that automatically activate during emergencies such as pandemics, elections, or natural disasters. These pre-established protocols ensure swift and decisive action to mitigate the spread of harmful misinformation, thereby protecting public trust and safety.

For example, during a natural disaster like a major hurricane, the government activates its crisis-specific misinformation framework. This framework includes the deployment of rapid-response teams trained to identify and address false information related to evacuation orders, shelter locations, and safety measures. Additionally, the framework imposes stricter penalties for individuals or groups that intentionally spread panic-inducing rumors. If a false report claims that a safe evacuation route is closed, the rapid-response team quickly verifies the information and disseminates accurate updates through official channels and social media. Meanwhile, those responsible for spreading the false report face heightened fines and legal actions. This proactive approach ensures that misinformation is swiftly countered, reducing confusion and enhancing the effectiveness of the emergency response.

e. Standards for verifiable content moderation

Recommendation: Standards for verifiable content moderation	Platforms should be required to use verifiable content moderation systems, such as third-party audits of their algorithms and moderation policies, ensuring that they are not inadvertently amplifying harmful content.		
	Why (?)	**What (!)**	**How (➔)**
	Auditing platforms ensure they comply with legal standards and helps to improve their methods of detecting and removing harmful misinformation.	Content moderation often lacks clear guidelines for auditing and verification.	Legislate mandatory third-party audits of social media platforms to assess the transparency and effectiveness of their content moderation systems.

To ensure that social media platforms effectively manage and mitigate the spread of harmful misinformation, it is essential to implement verifiable content moderation systems. This involves requiring platforms to undergo third-party audits of their algorithms and moderation policies, guaranteeing transparency and accountability in how content is handled. By mandating these standards, governments can ensure that platforms adhere to legal requirements and continuously improve their methods for detecting and removing misleading or dangerous information.

For example, a government passes legislation requiring all major social media and digital platforms to undergo annual third-party audits of their content moderation systems. An independent auditing firm is contracted to evaluate how algorithms prioritize or suppress content, the criteria used for removing misinformation, and the effectiveness of these measures in preventing the spread of false information. If a platform is found to be inadvertently promoting misleading health advice through its algorithm, the audit report will highlight these issues and recommend specific adjustments. Platforms that fail to comply with the audit requirements or do not implement the recommended changes face significant fines and potential restrictions on their operations. This approach ensures that content moderation practices are transparent, effective, and aligned with legal standards, thereby reducing the inadvertent amplification of harmful misinformation.

5. CONCLUSION

Addressing the widespread issue of misinformation requires a concerted effort grounded in well-defined strategies, norms, and standards. This report has provided comprehensive recommendations that nations can adopt to proactively combat misinformation. While the analysis of current approaches reveals a diverse landscape of efforts across national and international contexts, it also highlights significant gaps that must be addressed to ensure a more effective response.

The recommendations on strategies underscore the need for clear definitions, anticipatory frameworks, and cross-border cooperation to preemptively tackle misinformation. Proactive measures, rather than reactive approaches that arise in times of crisis, are essential for ensuring timely and accurate responses to the rapid spread of misinformation. Furthermore, the engagement of vulnerable populations is critical to reducing the impact of misinformation.

Proactive measures, rather than reactive approaches that arise in times of crisis, are essential for ensuring timely and accurate responses to the rapid spread of misinformation. Furthermore, the engagement of vulnerable populations is critical to reducing the impact of misinformation.

On the front of norms, it is vital that societies foster accountability both for individuals and platforms. The promotion of transparency and the incorporation of public education into the core values of digital governance are central to building resilience against misinformation. International collaboration and multi-stakeholder engagement also form key components of these norms, as the global nature of misinformation necessitates cooperative, cross-border solutions.

Lastly, the recommendations for standards highlight the importance of establishing clear, enforceable guidelines. These standards should include proportional penalties for misinformation, mandatory platform accountability, and specific measures for addressing emerging technologies such as AI and deepfakes. By setting these measurable benchmarks, nations can create consistent and transparent legal frameworks that ensure accountability and fairness in the digital space.

These recommendations on strategies, norms, and standards provide a roadmap for nations to strengthen their digital agendas and more effectively mitigate the societal dangers posed by misinformation. As misinformation continues to evolve, it is essential that policymakers and stakeholders implement these forward-thinking measures to safeguard public trust and promote a safe, informed digital ecosystem.

APPENDIX: Overview of laws to combat misinformation

This table presents a comprehensive review of key legislative measures aimed at combating misinformation. The table includes laws currently in force, some of the laws may have been amended or repealed. The authors have made their best efforts to collect and verify the accuracy of this information; however, given the dynamic nature of legal frameworks, some changes may have occurred.

Country	Law
Algeria	Penal Code, Law 20-06, Article 196
Angola	Penal Code, Article 224, Article 322
Australia	National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018
Australia	Foreign Influence Transparency Scheme Bill 2018
Azerbaijan	Law 30-VIQD - Amendments to the Law on Information, Informatization and Protection of Information
Bahrain	Press Law, Article 70 (c) Penal Code, Article 168
Bangladesh	Digital Security Act
Belarus	Article 22.9: Violation of Legislation on Mass Media and Amendments to Media Laws to Address Fake News
Benin	Digital Code (2018), Article 550
Bolivia	Decree 4200, Article 13-2 Decree 4231
Bosnia-Herzegovina	Decree, 032-2020
Botswana	Regulation 31(3) of the Emergency Powers (COVID-19) Regulations
Brazil	Electoral Propaganda Resolution TSE 23.551/2017
Burkina Faso	Law 044-2019/AN
Myanmar	Law amending the Electronic Transactions Law, Article 38c
Cambodia	Joint-Directive, Ministries of Interior, Telecommunications and Information Law on the management of the nation in emergencies
Cameroon	Law 2016/007 of the Penal Code, Sections 122 (1)(b), 122 (1)(g), 164 (1), 304, 305, 314
Canada	Bill C-76 (Elections Modernization Act), Section 91 (1), Section 92
Chad	Law on Electronic Communications 014/PR/2014 Law on Audiovisual Communication020/PR/2018 Law on Written Press and Electronic Media 025/PR/2018

China	Interpretation on Several Issues Regarding the Applicable Law in Cases of Using Information Networks to Commit Defamation and Other Such Crimes, Articles 5, 7, 9 People's Republic of China Criminal Law (amended 2015), Article 291-1 Administrative Provisions on Deep Synthesis of Internet Information Services, Article 6 Interim Measures for the Management of Generative Artificial Intelligence Services, Article 4
Costa Rica	Law 9048, Article 236
Cote d'Ivoire	Law 2013-451, Article 65
Cuba	Decree-Law 35, Article 15 (e), Article 69
Cyprus	Draft Law
Denmark	Law 269
Djibouti	Penal Code, Article 425
Egypt	Law on the Organisation of Press, Media and the Supreme Council of Media
Eswatini	COVID-19 Regulations, Article 29
Ethiopia	The Ethiopian Electoral, Political Parties Registration and Elections Code of Conduct Proclamation No. 1162/2019, Article 64 (5), 79 (3), 98 (1)(e), 130 (7), 144, 157 (3)(b) Hate Speech and Disinformation Prevention and Suppression Proclamation No.1185/2020
Fiji	False Information Act 2016
France	Law on the fight against the manipulation of information 2018-1202
Gabon	Law 019/2016, Article 44
Ghana	Electronic Communications Act, Section 76 Criminal Code, Section 208
Greece	Law 4855/2021, Article 36
Guinea	Law on Cybersecurity and Protection of Personal Data L/2016/037/AN
Hungary	Act XII of 2020 on the Contamination of Coronavirus, Section 337
Jordan	Defense Order (8) of 2020
Kazakhstan	Criminal Code, Article 274
Kenya	The Elections Offenses Act, Section 13 (b), 13 (j), 13 (k), 13 (l)
Kenya	The Computer Misuse & Cybercrimes Act, Sections 22, 23, 25, 38
Kuwait	Law 8 of 2016 Regulating Electronic Media, Article 17
Kyrgyzstan	Law on Protecting against False and Inaccurate Information
Laos	Decree 327 on Internet-Based Information Control/Management Ministerial Order (Lao Ministry of Information, Culture and Tourism and Government) 256

Lesotho	Communications Act; Broadcasting Rules Legal Notice 26 of 2020: Declaration of COVID-19 State of Emergency Notice, Article 3 (f) Public Health (COVID-19) Risk Determination and Mitigation Measures Regulations, Article 15 (7)
Madagascar	Law 2016-029 Establishing the Code of Media Communication, Articles 23, 30, 59
Malaysia	Anti-Fake News Act 2018 Emergency (Essential Powers) (No. 2) Ordinance 2021
Malta	Media and Defamation Act
Mauritania	Law 2020-015 on the Fight Against the Manipulation of Information
Moldova	Law on the Intelligence and Security Service of the Republic of Moldova Law 64 / 2010 on freedom of expression
Mongolia	Criminal Code, Article 13 (14)
Morocco	Law No. 22.20 on the use of social networks, open broadcasting networks or similar networks (Withdrawn)
Namibia	Regulations published under Proclamation No. 9 of 28 March 2020, Article 16 (1)(c)
Nepal	National Penal Code, Article 84
Nicaragua	Special Cybercrime Law, Article 30
Niger	Cybercrime Law, Article 9
Nigeria	Cybercrimes (Prohibition, Prevention, etc) Act, Article 14 (2) Broadcasting Code of Conduct, Articles 3.3, 3.5, 5.6, 7.3
Oman	Royal Decree 96/2011 (Amendments to the Omani Penal Code Articles 135, 182)
Pakistan	Citizens Protection (Against Online Harm) Rules
Philippines	Revised Penal Code (Republic Act 10951), Article 154 (1) Bayanihan to Heal as One Act (Republic Act 11469), Section 6 (f)
Qatar	Cybercrime Prevention Law Crimes against Internal State Security Section of the Penal Code, Article 136 bis
Romania	Decree 195 on the Establishment of a State of Emergency in the Territory of Romania, Article 54
Russia	Russian 2019 Fake News Laws COVID-19 Fake News Law (Amendments to the Criminal Code and to the Code of Administrative Offences) Fake News Law
Rwanda	Law 60/2018 on Prevention and Punishment of Cyber Crimes, Article 39 Law 68/2018 Determining Offences and Penalties in General, Articles 132, 194
Saudi Arabia	Anti-Cyber Crime Law, Article 6 (1)

Senegal	Penal Code, Article 255
Sierra Leone	Cyber Security and Cyber Crime Act, Articles 42 (3), 44 (2)(b)
Singapore	Protection from Online Falsehoods and Manipulation Bill
Somalia	Media Amendment Act, Articles 4.1-t, 29
South Africa	Regulations Issued in Terms of Section 27(2) of the Disaster Management Act, Section 11 (5)
Sri Lanka	Penal Code, Section 120 Police Ordinance, Section 98
Sudan	Cybercrimes Law, Article 24
Syria	Law 20 of 2022
Taiwan	Special Act for Prevention, Relief and Revitalization, Measures for Severe Pneumonia with Novel Pathogens, Article 14 Anti-Infiltration Law
Tajikistan	Administrative Code, Article 374 (1)
Tanzania	Electronic and Postal Communications (Online Content) Regulations, Thid Schedule (10)
Thailand	Computer Crime Act, Sections 14 (1), 14 (2), 14 (5)
The Gambia	Criminal Code, Article 114
Togo	Penal Code, Article 497 Law 2018-026 on Cybersecurity and the Fight Against Cybercrime, Article 25 Law 2020-001 Relating to the Press and Communications Code, Articles 35, 36, 37, 153
Turkey	Law on the Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of such Publications 5651
Uganda	Uganda Communications Act, Schedule 4 Data Protection and Privacy Act, Article 15 (2) Content Regulations Computer Misuse Act, Section 26 (C)
United Arab Emirates	Government resolution (COVID-related)
United States of America	Countering Foreign Propaganda and Disinformation Act
Uzbekistan	Law on Informatization, Article 12 Penal Code, Article 244
Vanuatu	Bill for the Statute Law Act 2 of 2021, Articles 120, 121
Vietnam	Cyber Security Law, Articles 5 (1)(i), 8 (1)(d) COVID-19 Misinformation decree
Zimbabwe	Public Health (COVID-19 Prevention, Containment and Treatment) Regulations, Section 14

Follow Us on

www.dco.org