# Multilateral Efforts on Information Integrity: Why a Clear Definition Is Needed


**Kamya Yadav, Alicia Wanless, and Samantha Lai**

**Abstract** How should "information integrity" be understood in the context of the information environment? The term has seen increased use by researchers and policymakers, yet its relative newness means that there is a lack of consistency in its definition and scope. This chapter provides analysis on how "information integrity" has been defined across multilateral efforts and existing literature. Using John Gerring's framework for "conceptual goodness", it evaluates how existing conceptualizations of the term falls short and provides guidance on how information integrity can achieve conceptual goodness. Only by doing so can information integrity fulfill its potential in supporting multi-stakeholder coordination to improve the global information environment.

## 1 Introduction

"Information integrity" is increasingly used by researchers and policymakers alike as a concept that democracies should pursue in the context of developing a healthy global information environment. Indeed, at least eight multilateral initiatives have been launched since 2018 on strengthening media literacy, countering disinformation, encouraging social media platforms to improve their operations and more—all under the umbrella of enhancing "information integrity." The U.S. Secretary of State, Anthony J. Blinken, mentioned some of these in a speech on the theme on March 18, 2024 (Blinken, 2024). These efforts all appear to be part of a larger initiative to move beyond the study of "disinformation," an increasingly politicized term (Napoli, 2025). However, in order for "information integrity" to have meaning,

K. Yadav
University of California, Berkeley, Los Angeles, CA, USA
e-mail: kamyayadav@berkeley.edu

A. Wanless · S. Lai (✉)
Carnegie Endowment for International Peace, Washington, DC, USA
e-mail: alicia.wanless@ceip.org



L. Ginsborg, P. Gori (eds.), *Disinformation*,
https://doi.org/10.1007/978-3-032-00480-2_25

more work needs to be done on developing a consistent definition and scope. Only by doing so can democracies achieve a more systemic understanding of how they can best govern their information ecosystems.

Currently, many draw on the criteria adopted by early users of the concept in the field of information security, where the goal of ensuring information integrity, whether in a closed computer system or interconnected network, is achieved by the application of controls and processes enabling the accuracy, reliability, and consistency of data. Most have added various conditions, from trustworthiness to plurality, but seldom uniformly (Matasick et al., 2024; WLA-CdM, 2018; ASD, 2023).

Different attributes in defining "information integrity" are undoubtedly needed for multilateral initiatives using the term as applied to a broader information environment as opposed to a closed, single computer system. A lack of consistency in those criteria, however, raises questions about the conceptual goodness of information integrity. Conceptual goodness matters as, without it, "information integrity" would not be used or understood consistently in policy and practice. That would lead to the misuse of the term, particularly in countries that have a history or are currently backsliding into authoritarianism. Moreover, without clarity and consistency, "information integrity" will continue to be conflated with narrower concepts such as "disinformation", thus reducing the utility of its application in policy, or indeed adoption at all, given the politicization of the latter. This chapter analyzes how "information integrity" has been applied in multilateral efforts and conducts a literature review to assess how current definitions used by government, academic and civil society actors measure against Gerring's framework of "conceptual goodness" (Gerring, 1999). We highlight the need for information integrity to move beyond the quality of information to include the production, consumption, dissemination, and governance of information. We conclude by providing suggestions for how information integrity might achieve conceptual goodness when applied to the information environment in the context of democracy.

What makes a concept good? John Gerring set out to answer this question in his eponymous paper, in which he outlined eight criteria for "conceptual goodness" (Gerring, 1999). For Gerring, a good concept is one that is familiar and resonates with a target audience, is short and coherent while distinguishing between similar ideas and drawing on shared definitions, and ultimately has both theoretical and field utility. How well does the concept of information integrity stand up to this analytical scrutiny?

"Information integrity" is not a new term, first becoming prevalent in the late twentieth century (Becker, 1983; Date, 1997). It was coined by scholars in the field of information security to evaluate the quality of information in a limited system, like that of an organization's database or computer system. The term is often used interchangeably with data quality, data integrity, and information quality. However, Boritz (2005) draws the distinction between "data integrity" and "information integrity," arguing that "data integrity" refers to a narrower concept as data is the "raw material" used to create a "finished information product." Scholars initially took on a wide-ranging approach to measuring information quality, with a survey by Delone and McLean (1992) reporting the use of 23 different measures. Yet, most

agreed on the core criteria for assessing "information integrity" (Mandke, 1996; Boritz, 2005): the accuracy, reliability, and consistency of information stored and accessed within a specific system. Specific definitions for each of these criterions will be discussed in more detail later in the chapter.

The term has since been adapted for use in more qualitative contexts. In library sciences, for example, "information integrity" refers to the need to address plagiarism and the manipulation of original records (Seadle, 2018). Researchers in media studies refer to "information integrity" as a way of evaluating information online (Shaker, 2006; Grabe & Bucy, 2022). More recently, the term has been applied more broadly in democratic societies to describe everything from efforts combating disinformation on digital spaces, to suggestions for improving countries' resilience in the broader information environment (UN, 2023; Adam et al., 2023).

## 2 "Information Integrity" in Multilateral Efforts

The use of "information integrity" in multilateral fora marks a collective recognition that citizens within democracies need to be able to access reliable information. This objective was consistently named across initiatives led by multilateral institutions (UN, 2023; UNDP, 2022; Matasick et al., 2024) and those led by coalitions of governments (WLA-CdM, 2018; MSI-INF, 2022; ASD, 2023; GAC, 2023). The information environment is global, and therefore concepts related to its governance even of national information ecosystems within it, should be international in nature. As per Wanless et al. (2025):

> Information ecosystems form where humans develop and use tools to process information into outputs that can be shared as a means of communicating with each other. In a sense, information ecosystems are communities bound by shared ideas—like the concept of a nation state, identity, or organization—and connected via technologies, from alphabets to artificial intelligence, that enable them to produce and share content…Information ecosystems are surrounded by a global information environment, which includes all the other human-made systems or constructs that impact them, such as economy, education, and politics.

Thus, this chapter focuses on definitions used by multilateral institutions, which by nature of their structure could lead to shared definitions of information integrity across multiple countries if not internationally.

Multilateral efforts identified that information integrity is necessary for citizens to trust institutions and make well-informed political decisions, both of which are essential cornerstones to democratic societies. To uphold information integrity, multilateral organizations proposed a range of multistakeholder, cross-sectoral efforts. However, the coordination of these efforts requires a clear definition for information integrity in order to translate understandings of the term into effective policy action.

### *2.1 Multilateral Institution-Led Efforts*

"Information integrity" is currently used by several multilateral organizations, including the United Nations (UN), the United Nations Development Programme (UNDP), and the Organisation for Economic Co-operation and Development (OECD).

The UN has been using the term "information integrity" chiefly in its pursuit of Global Principles for Information Integrity (UN, 2024).[1] The term was first invoked in "Our Common Agenda Policy Brief 8: Information Integrity on Digital Platforms," in which the secretary-general called for a code of conduct on information integrity. In the policy agenda, "information integrity" was defined as "the accuracy, consistency, and reliability of information" (UN, 2023, 5). The effort focuses on the online space and what member-states, social media platforms, and other stakeholders can do to improve the integrity of information [2]. This includes improving regulatory responses, increasing data access for researchers, disincentivizing the spread of disinformation, empowering users, bolstering independent media, and future-proofing emerging technologies [16–19]. The principles underlying the proposed code also include commitments to respect human rights, increase transparency, and enhance trust and safety [21].

Following the publication of "Our Common Agenda," the United Nations Educational, Scientific, and Cultural Organization (UNESCO), another UN agency, released 'Guidelines for the Governance of Digital Platforms,' which was intended as a complementary set of principles to the UN policy brief that specifically address digital platform governance. These guidelines "seek to contribute to and be informed by ongoing UN-wide processes, such as the implementation of the proposals in 'Our Common Agenda.'" The document made no mention of information integrity and focused primarily on the online space.

The call for a code of conduct in 'Our Common Agenda' culminated in the development of the United Nations Global Principles for Information Integrity, published in 2024. Information integrity there refers to an ecosystem "where freedom of expression is fully enjoyed and where accurate, reliable information, free from discrimination and hate, is available to all in an open, inclusive, safe and secure information environment" [3]. It proposes five principles for information integrity, namely: improving societal trust in information and developing resilience to disruption or manipulation [8]; creating healthy incentives in digital advertising models [10]; empowering individuals to have control over their online experiences through access to diverse and reliable sources of information [12]; maintaining independent,

[1] The adoption of the term information integrity built on early UN efforts, including *Disinformation and freedom of opinion and expression: report of the Special Rapporteur on the Promotion and Protection of the Rights to Freedom of Opinion and Expression* (Khan, 2021) and *Countering disinformation and promotion and protection of human rights and fundamental freedoms: resolution / adopted by the General Assembly* (UNGA, 2021).

free, and pluralistic media [14]; and increasing transparency by technology companies to improve researcher data access [16].

"Information integrity" has also been used by the United Nations Development Programme (UNDP), a UN agency, since 2021. UNDP has actively championed "information integrity" and developed a framework for assessing it (UNDP, 2022). UNDP identified the lack of "internal clarity as to what this area of work entails, why it is important to UNDP and how it can translate into programming" (UNDP, 2022). To bring clarity to the use of "information integrity," the UNDP defined the term not just around the criteria of accuracy, consistency, and reliability of information but also the processes and systems within the information environment. Moving beyond the UN focus on online information, UNDP's definition of "information integrity" "requires citizen access to trustworthy, balanced and complete information on current affairs, government actions, political actors and other elements relevant to their political perceptions and decision-making" (UNDP, 2022, 4).

The Organisation for Economic Co-operation and Development (OECD)'s DIS/MIS Resource Hub aims to support member countries in "tackling disinformation and strengthening information integrity" through a shared learning approach (OECD, n.d.-a). The hub emerged from an OECD Expert Group on Governance Responses to Mis- and Disinformation and is co-chaired by France and the United States. The hub follows a three-pronged framework to design policy options to counter disinformation and promote information integrity—promote transparent and healthy information spaces; strengthen societal resilience; and reinforce accountable, transparent, and agile governance (OECD, n.d.-b). In a recent report by the hub, they defined "information integrity" "as information environments that are conducive to the availability of accurate, evidence-based, and plural information sources and that enable individuals to be exposed to a variety of ideas, make informed choices, and better exercise their rights" (Matasick et al., 2024). At the time of writing, the OECD was undertaking a public consultation on their concept of information integrity.

## *2.2 Country-Led Multinational Efforts*

"Information integrity" has also been used to frame several country-led multinational efforts, from roundtables to global declarations.

In 2018, the Ministry of Foreign Affairs of the Republic of Latvia led the Roundtable on Global Governance for Information Integrity, which included former political leaders from Mongolia, Tunisia, and Austria. Based on the discussions at the Roundtable, the World Leadership Alliance-Club de Madrid (WLA-CdM) released a report, which defined "information integrity" "as the trustworthiness, balance and completeness of information to which citizens have access on current affairs, government actions, political actors and other elements relevant to their political perceptions and decision-making" (WLA-CdM, 2018, 4). Policy recommendations in the report included establishing a bill of digital rights; regulating the

digital environment; encouraging voluntary action by online platforms to increase transparency, reduce anonymity, and diversify content; supporting the publication of reliable information; and educating citizens.

The Council of Europe established the Committee of Experts on the Integrity of Online Information in 2022, which has since convened 13 members from seven European Union states (Croatia, the Netherlands, Poland, Romania, Switzerland, the United Kingdom, and Greece) and six independent observers from academia and civil society (MSI-INF, 2022). Its guidance notes in December 2023 focused on countering disinformation through fact-checking and did not offer a definition of "information integrity" (MSI-INF, 2023a).

Also beginning in 2022, Canada and Latvia, with the Alliance for Securing Democracy (ASD) at the German Marshall Fund (GMF), have co-convened the Summit for Democracy Cohort on Information Integrity. In its follow-on report, ASD noted, "Information integrity is fundamental for democracy. Access to reliable, accurate, and impartial information is essential for public trust and civic engagement, good and effective governance, healthy democratic discourse, and informed decision-making" (ASD, 2023, 3). The summit centered around two key action points—creating four working groups, each addressing an issue related to information integrity and a global mapping project that tracked organizations and initiatives involved in information integrity activities (ASD, n.d.).

Last but not least, building on the Summit for Democracy and aiming to complement the Code of Conduct, Canada, and the Netherlands launched the Global Declaration on Information Integrity Online in September 2023 (GAC, 2023). The declaration constitutes high-level international commitments for signatory governments to voluntarily ensure the integrity of information online. The declaration defines "information integrity" "as an information ecosystem that produces accurate, trustworthy, and reliable information, meaning that people can rely on the accuracy of the information they access while being exposed to a variety of ideas." Commitments are rooted in international and human rights law and focus on multiple stakeholders, including civil society, industry, regulatory bodies, and academia. They include responses to generative artificial intelligence, diversifying online content, improving online civic education, protecting minorities from disinformation, fact-checking, increased trust and safety by platforms, and more. As of September 2023, the declaration has 34 signatories. Most signatories are from Europe and North America, while some are from Latin America, the Caribbean, Asia-Pacific, and Africa.

## 3 Dissecting Definitions of "Information Integrity"

### *3.1 "Information Integrity" as Defined in Multilateral Efforts*

Of the eight multilateral initiatives outlined above, six provided definitions of "information integrity" in related outputs. Five of these initiatives drew on the definition of "information integrity" used in information security. Of those initiatives,

only the UN's 2023 publication "Our Common Principles" used the exact attributes of accuracy, consistency, and reliability (UN, 2023).[2] The use of attributes from information security's definition of "information integrity" ranged on the high end, with the UNDP and the UN's 2023 definition using all three to the OECD drawing on only one criterion—accuracy (UN, 2023; UNDP, 2022; Matasick et al., 2024).

Most multilateral organizations modified the definition of "information integrity" used in information security and developed additional attributes for their concepts. However, some definitions conflated what constitutes the integrity of information (i.e., attributes describing its state) with the desired outcomes of pursuing information integrity (i.e., as a public good, for example). This confusion makes pursuing coherent policy and practical applications of the term more challenging. An initiative that avoids that confusion is the UN's definition in "Our Common Principles", in which "Information integrity refers to the accuracy, consistency and reliability of information," may be interpreted as a desired state of the digital information ecosystem achieved through regulatory, digital literacy, and other relevant interventions by both domestic and international stakeholders (UN, 2023). This clarity is critical, in particular, due to the multilateral and multistakeholder context of the UN system. The diverse socio-economic and political conditions of UN member-states constitute significant challenges on the road to achieving sustainable information integrity on a global scale. In comparison, their revised definition of information integrity in their Global Principles is not as clear (UN, 2024). The definition laid out the desired criteria for information (accurate, reliable, open, inclusive, safe, and secure) but also listed in the same sentence what that information should help people do ("freedom of expression is fully enjoyed, free from discrimination and hate, is available to all"). The OECD's report presented a similar issue, where desirable qualities of information ("accurate, evidence-based, and plural") were included alongside what information integrity was meant to achieve ("be exposed to a variety of ideas, make informed choices, and better exercise their rights") (Matasick et al., 2024). Both the OECD's approach and the UN's new approach underscores a lack of understanding in distinguishing between the quality of information and the desired outcomes of information integrity, which muddies the definition and, by extension, makes it difficult to operationalize through policy and practice-making. There is a need to distinguish terms explicitly related to the quality of information (attributes) from the additional terms (desired outcomes).

There was some consistency in additional attributes beyond "accuracy, consistency, and reliability" listed by multilateral organizations. The attribute that information should be balanced or impartial appeared in three definitions, whereas that of completeness of information was included in two. The OECD uniquely added one more attribute, which is that information should be evidence-based. The most commonly desired outcomes—"access" or "availability" of information—appeared

[2] While the World Bank has referenced scaling up "information integrity" in the context of its Global Data Facility, this effort appears to use the term in a more traditional information security sense, than the initiatives discussed here. Given that nothing more than a passing reference was made, we have chosen to leave this usage out of analysis. See: Fu et al. (2022).

in five concepts of information integrity. While "availability" tests the categorical boundaries between "attribute" and "outcome," it denotes a quality related to the process of people's ability to consume information, pushing it toward a desired result. In other words, information being available means little if people are not consuming it. Another commonly desired outcome, appearing in four definitions, was information integrity's role in ensuring citizens can make informed choices. A few outcomes appeared only once, such as the aim for information integrity to help citizens "better exercise their rights" (Matasick et al., 2024) and ensure "civic engagement, good and effective governance, healthy democratic discourse" (ASD, 2023).

Trust and plurality appeared both as attributes and desired outcomes across definitions, further blurring the lines in a wider concept of information integrity. The notion of trust appeared both as an attribute for information (UNDP, 2022; WLA-CdM, 2018), as well as an outcome among the public in definitions of "information integrity" (ASD, 2023). This included the Global Declaration, which didn't mention trust specifically, but spoke of the need for citizens to be able to "rely" on information. The idea that information should come from many sources or have plurality was also an attribute (Matasick et al., 2024), as well as a desired outcome in that citizens should be "exposed to a variety of ideas" (Matasick et al., 2024; WLA-CdM, 2018).

| Organization/ initiative | Definition of information integrity |
|---|---|
| UN: Our Common Agenda (UN, 2023) | "Information integrity refers to the **accuracy**, **consistency** and **reliability** of information" |
| UN Global Principles for Information Integrity (UN, 2024) | "The integrity of the information ecosystem — where freedom of expression is fully enjoyed and where **accurate**, **reliable** information, **free from discrimination and hate**, is available to all in an **open**, **inclusive**, **safe** and **secure** information environment" |
| UNDP (UNDP, 2022) | "Information integrity is determined by 'the **accuracy**, **consistency**, and **reliability** of the information **content**, **processes** and **systems** to maintain a **healthy** information ecosystem.' It requires citizen **access** to **trustworthy**, **balanced** and **complete** information on current affairs, government actions, political actors and other elements relevant to their **political perceptions** and **decision-making**" |
| OECD (Matasick et al., 2024) | Information integrity is "defined as **information environments** that are conducive to the **availability** of **accurate**, **evidence-based**, and **plural** information sources and that enable individuals to be exposed to a **variety of ideas**, make **informed choices**, and **better exercise their rights**" |
| Roundtable on Global Governance (WLA-CdM, 2018) | "Information integrity as the **trustworthiness**, **balance** and **completeness** of information to which citizens have **access** on **current affairs**, **government actions**, **political actors** and other elements relevant to their **political perceptions** and **decision-making**" |
| Summit for Democracy (ASD, 2023) | "Information integrity is fundamental for democracy. **Access** to **reliable**, **accurate**, and **impartial** information is essential for **public trust** and **civic engagement**, **good and effective governance**, **healthy democratic discourse**, and **informed decision-making**" |

| Organization/ initiative | Definition of information integrity |
|---|---|
| Global Declaration (GAC, 2023) | "The term 'information integrity' is defined... as an **information ecosystem** that produces **accurate**, **trustworthy**, and **reliable** information, meaning that people can **rely** on the accuracy of the information they **access** while being exposed to a **variety of ideas**" |

Some definitions delineated boundaries around types of information for which integrity was sought. This was distinct from both the attributes of information integrity and its desired outcomes. These subject areas included information on "current affairs, government actions, political actors and other elements relevant to their political perceptions and decision-making" (UNDP, 2022; WLA-CdM, 2018).

Many of these definitions attempted to adapt the term for broader use beyond the scope of a limited computer system, from which the term "information integrity" originally emerged. This includes the four initiatives that took a decidedly online-only focus (UNDP, 2023; WLA-CdM, 2018; GAC, 2023; MSI-INF, 2022). The Global Declaration and OECD diverged from the traditional definition relating to the quality attributes of information integrity, to position information integrity as a positive vision (objective) for "an information ecosystem" or "information environments" (GAC, 2023; Matasick et al., 2024). UNDP mentioned the "content, processes and systems [needed] to maintain a healthy information ecosystem" (UNDP, 2022). While the UN's "Our Common Agenda" referred exclusively to information integrity in the online space, the Global Principles included offline elements such as societal trust and free media as component parts for information integrity (UN, 2023, 2024). Indeed, four of the definitions apply firmly to the information environment as a desired end state in democratic societies. There are similarities in intent across initiatives. However, proposed ways to achieve information integrity varied across efforts, from fact-checking primarily conducted in online spaces (MSI-INF, 2022) to wider efforts to evaluate how a country's political and societal conditions affect the state of their information ecosystems (UNDP, 2022). The lack of shared definitions and outcomes hinders efforts by multilateral fora to achieve their stated goals, as it leads to disorganized or even conflicting efforts in policy development, resourcing, and capacity-building. This has not yet been an issue in work related to information integrity, which remains a relatively new field. However, one can easily imagine a scenario where one initiative demands more regulation around the accuracy of content produced by media outlets, while another advocates for the ability of outlets to produce content without facing any political restrictions. A clear definition can help initiatives navigate these conflicts and coordinate existing efforts.

The information environment is the place where people process information to make sense of the world, encompassing humans, technology, and content, as well as the relationships between them (Wanless et al., 2025). The information environment is integral to the legitimacy of democracy, which is based on citizens making free and informed decisions. This means that if "information integrity" is to become a guiding principle for democracies, it must cover more than the quality of information. It must include the production, consumption, dissemination, and governance

of information, which, in turn, includes aspects of humans and their cognition. And, moreover, for information integrity to be achieved across multiple democracies, a functional definition must emerge that is shared across stakeholders. How might that be achieved? What can be learned from definitions of "information integrity" elsewhere?

### *3.2 "Information Integrity" as Defined by the Wider Field*

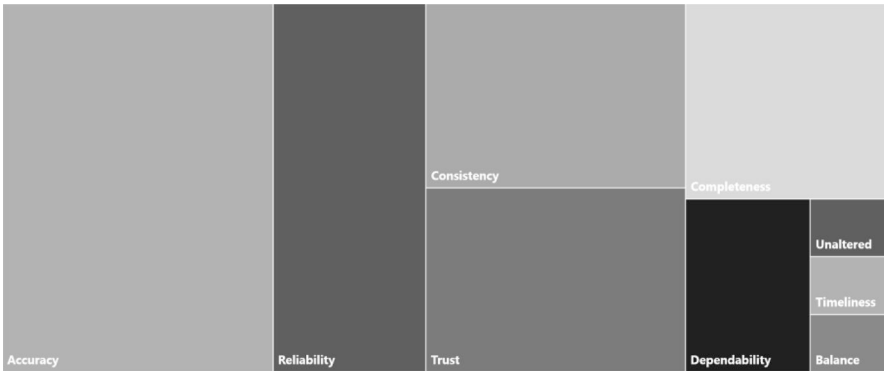
The variance in how multilateral initiatives define "information integrity" mirrors the situation in the wider field, as we demonstrate in a review of 48 documents mentioning "information integrity" published between 2000 and early 2024. These documents include those published in relation to the multilateral initiatives already mentioned, along with others from academia and civil society. They comprised 16 papers in academic journals, 16 reports, 10 articles, three conference papers, two webpages (from the UN and Council on Europe, respectively), and one book. The documents were published by stakeholders across sectors, including academia (20), civil society (12), government or multilateral organizations (11), and industry (5). They were found using Google Search, publicly accessible to be analyzed, and predominantly consisted of material defining the term or making it actionable, which is best described as referring to policy or practice, including one from the Chartered Professional Accountants, Canada (2019). For those papers where clear disciplines could be identified, they came from the fields of information security (16), library sciences (2), media studies (2), health care (2), and finance (2).

The majority of these documents (44%) situated "information integrity" in the context of a limited information system, such as healthcare records, a company's information technology infrastructure, or financial security. Just under one-third (29%) framed it in the context of the wider information environment, and 25% did so in relation to information circulated online. One outlier positioned "information integrity" in the context of research (Seadle, 2018).

In total, 30 out of 48 documents defined "information integrity," and those are the basis for the following analysis. All 5 documents from industry included definitions. Of the 22 academic documents analyzed, 14 included definitions and 6 did not. Across documents produced by governments and multilateral organizations, 6 out of 11 included definitions; while in civil society, the numbers fell to 5 out of 12.

The majority (77%) of the definitions drew entirely (e.g., Khan et al., 2013) or partially on the three attributes derived from the information security concept: accuracy, consistency, and reliability of information. For example, Adam et al. listed the attributes of "consistency, reliability, accuracy, fidelity, safety, and transparency" for information integrity (2023). Some avoided the original attributes entirely and developed new concepts, such as "Information integrity can be defined in three contexts: data modification, information flow, and quality-related" (Harley & Cooper, 2021).

Of the 23 papers that drew on the original criteria, 13 contributed further factors, for a total of 36 different criteria across documents. Accuracy was the most used criterion, mentioned in 23 definitions of "information integrity", followed by reliability (13), trustworthiness (11), consistency (11), completeness (8), dependability (5), and representational faithfulness (4). Balance, timeliness, and unaltered were all included three times. A few attributes were mentioned twice, such as authorized, currency, safety, timeliness, transparency, truthfulness, and validity. A majority of attributes (20) were mentioned only once. This suggests that while there is consistency in the core concepts originating from information security, authors diverge when adapting the original definition in relation to their field of practice.




While half of all definitions offered added new attributes, very few explained what each attribute meant. In fact, just six of the thirty documents offered further clarification on what was meant by each attribute in a definition of "information integrity", with all but one of those coming from academia, specifically information security. (Bovee et al., 2003; Boritz, 2005; Nayar, 2007; Khan et al., 2013; Boritz & Datardina, 2019; Adam et al., 2023). Drawing from those definitions, only 'accuracy' was more or less consistently defined across the six concepts, roughly meaning that the information is free from errors or too much deviation from a standard starting point. Consistency was included in just four of the definitions where attributes were described, two of which touched on the idea of expecting similar results across time from information (Bovee et al., 2003; Nayar, 2007). A fourth attribute—completeness—was mentioned across four concepts to refer to information existing in its original totality (Bovee et al., 2003; Boritz & Datardina, 2019) or relating to its representational fullness in accordance with whatever the information is supposed to convey (Boritz, 2005). Accuracy aside, these attributes were inconsistently defined across concepts. Reliability of information is listed as an attribute in three of the six concepts, with some adding sub-attributes of reliability, such as currency, completeness, and traceability of information (Nayar, 2007) and others referring to reliability as what a user expects, which is more like a desired outcome. (Khan et al., 2013).

"Information integrity" originated from information security and adopted into other disciplines such as health care, finance, and library sciences. However, the field working on the information environment cannot readily transfer the definition provided by information security, as the information environment is not a closed system. Information flows across different platforms. The information that individuals receive, in addition to their interpretations of what they absorb, differs. As a result, a definition of "information integrity" applicable to the information environment also needs to account for the underlying infrastructures and means that enable the flow of information, their ownership, possible political implications of control and the differences in how people receive and interpret it, among many other important considerations. In a company, information accuracy can be achieved by applying specified controls and processes aimed at ensuring its correctness. In the information environment, however, it is not just about whether information has been corrected but also how it has been corrected, who corrected the information, and how both the original and corrected information were received by audiences. The existing use of 'consistency' from information security also falls short. Depending on their levels of access to independent media or the internet, individuals can be exposed to vastly different kinds of information and, as a result, come to "inconsistent" conclusions on the same topic. Similarly, in the context of the information environment, the existing definition of reliability is inadequate, as it is not enough that the information is complete but that it is also understood by audiences as intended. In short, the complexities of the information environment and democracy demand a more precise and elaborate definition of "information integrity."

Of all the analyzed documents in this study, only one provided definitions for how the attributes applied in the information environment (Adam et al., 2023). This report attempted to update the primary three attributes of "information integrity", specifically in the context of responding to crises in the information environment. Thus, the attributes became a mix of what might be desired from information itself as well as its processing, with accuracy relating to the correctness and reliability to the suitability of information, whereas consistency pertaining to the steady access to such information. To this, three more attributes were added. Fidelity could be applied both to the information in the degree of exactness in its reproduction or the "degree to which audiences understand information as originally intended by the producer/sender." The attribute of safety was applied to the process of people accessing information, that it should be free from risk or injury, whereas transparency applied to the openness and traceability of both information and the processes by which various stakeholders engaged in information integrity initiatives. While imperfect, this attempt speaks to the need to review not just concepts of information integrity but also the accompanying attributes for application to the broader information environment.

Not only should the most commonly used attributes to define "information integrity" be revisited in the context of the information environment but consensus and definitions must also be built on what further criteria will be added. This is key given the role the information environment plays in the legitimacy of democracy and, indeed, the suggested aims of multilateral efforts in existing definitions of

"information integrity" to ensure that citizens are able to make free and informed decisions. Many of the efforts explored above were inherently multistakeholder, engaging governments, civil society, and industry in a response that would impact citizens. This makes it crucial that a shared definition of "information integrity" is developed to clarify precisely what is meant by each criterion being adopted.

## 4 The Conceptual Goodness of Information Integrity

Given the lack of consistency in defining "information integrity" in a manner that makes it immediately useful for policymaking and practice in the context of the information environment, we use Gerring's framework of conceptual goodness to identify attributes which could constitute a more universal definition (Gerring, 1999). Assessing against Gerring's eight criteria for conceptual goodness, the original and shorter definition of "information integrity" from information security based on the accuracy, reliability, and consistency of information might stand the test. However, emerging definitions of information integrity in the context of the information environment need to be better understood. At a minimum, there is a need to differentiate between conflating information with the information environment. Further elaboration of information integrity's attributes will also be required to better position this concept as a cornerstone of government and multilateral policy development. How can this be achieved in a way that ensures the conceptual goodness of information integrity?

### *4.1 Familiarity: How Familiar Is the Concept (to a Lay or Academic Audience)?*

Gerring's first criterion is that the concept must "fit between new and old meanings" [368]. In the literature reviewed, "information integrity" defined by using three core attributes of accuracy, reliability, and consistency, was first introduced in information security in the 1970s and has gradually been adopted by academics across fields, from library sciences to media studies, and, more recently, by governments and multilateral organizations. In this regard, it is increasingly familiar to several audiences. At its core, based on these three attributes, "information integrity" appears to be a common way to describe an ideal state of information, be it in a closed computer system or a democracy. However, as the concept develops and further attributes are added, information integrity risks sounding familiar but meaning very different things depending on the audience using it. Moreover, the variation and continued adding of new attributes, as well as desired outcomes from achieving those attributes, will render newer concepts of information integrity less and less familiar for those using older definitions—not to mention how much harder it will

make for lay people to become familiar with the term. In the literature reviewed, where definitions of "information integrity" in the context of the information environment have built on the original definition using the attributes of accuracy, reliability, and consistency, there is a greater likelihood that the concept will be familiar to those who have used it.

### *4.2 Does the Chosen Term Ring (Resonate)?*

Given its adoption across sectors and fields, the original concept of information integrity has the potential to resonate with a broader audience. Based on the documents examined, integrity evokes a high standard based on principles. Still, for information integrity to be acceptable as a meaningful concept by democracies, users of it should take care to articulate what those corresponding principles might be. Some multilateral initiatives have attempted to draw that connection. The Global Declaration cites Article 17 and Article 19 of the International Covenant on Civil and Political Rights (ICCPR) and the United Nations Guiding Principles on Business and Human Rights (GAC, 2023). The United Nations, meanwhile, points to the Universal Declaration of Human Rights and the ICCPR (UN, 2023). Multilateral fora can build on this work by defining goals of information integrity and identifying redlines that governments should not cross in upholding it. Moreover, given that "information" is itself a contested term, meaning many things to different people, corresponding definitions for what that entails are also encouraged (Wanless, 2023). In this regard, some of the definitions put forward by multilateral initiatives are heading in the right direction (UNDP, 2022; WLA-CdM, 2018), but for clarity's sake, there should be a separation between defining information integrity as an end state/objective and the types of information that would require information integrity, be it information on politics, health, or entertainment.

### *4.3 How Short Is (a) the Term and (b) Its List of Defining Attributes (the Intension)?*

Gerring argues that "good concepts do not have endless definitions" and that "it should be possible to say what it is one is talking about without listing a half-dozen attributes" [371]. In that regard, the original definition from information security is concise. The challenges arise when the concept is morphing as others adopt it and more attributes are added. Of the documents analyzed, just a third of those that offered definitions used all three of the original attributes, and half of those (unsurprisingly) came from the information security field. However, as the concept of information integrity morphs, it is increasingly becoming a list of its attributes or component parts. The definition with the fewest attributes contained only one:

"Information integrity refers to the degree in which a piece of information is true or honest" (Rügenhagen et al., 2020). Two definitions contained seven attributes each. (Trites, 2013; Adam et al., 2023). The attribution creep isn't isolated to those documents in our data set and plagued much earlier concepts of information integrity, with some using up to 23 criteria to define the quality of information (Delone & McLean, 1992), making the concept less parsimonious.

Beyond attributes, however, newer definitions include the desired outcomes of pursuing information integrity as part of the concept. This was the case for all the definitions used by the multilateral initiatives discussed above, except for the UN's definition proposed in 2023. Still, it comes with the risk of muddying the concept. For the sake of clarity, concepts of information integrity should be focused on the attributes of the concept itself and separated from the aims of pursuing it. Keeping the definition of information integrity concise and focused could help reduce confusion and thus mitigate the chances of it being politicized. This is all the more important given the complexity of the information environment and the need for adoption of the concept of "information integrity" across as many countries as possible.

## *4.4 Coherence: How Internally Consistent (Logically Related) Are the Instances and Attributes?*[3]

The degree to which attributes were internally consistent varied across definitions, and it became more difficult to discern where concepts did not provide further explanation about what was meant by various attributes. At a minimum, accuracy, which means information is free from errors or deviation, and consistency, which means information remains the same across time, can be seen to logically relate to each other. However, the inconsistency in which attributes were used or defined across usages makes the concept of information integrity less coherent.

Here, the information security approach presents the same conflation between attributes and objectives, with some definitions distinguishing between the integrity of information and the integrity of the system (Flowerday & Von Solms, 2005) and others mixing the two to define "information integrity" (Nayar, 2002, 2007; Geisler et al., 2003; Sinnett, 2008). The mixing of the state of information (integrity of data) and the system (system integrity) might make sense in the context of a controlled and confined system, but when applying "information integrity" to the wider information environment, a distinction should be made between the two to better ensure conceptual coherence, given the increasing complexity.

Definitions that expand "information integrity" to the integrity of the wider system in which the information exists present an additional challenge (UNDP, 2022;

[3] "Instances" refer to a term's instances of use. "Attributes" refer to qualities commonly associated with the term. For this piece, "instances" refer to the use of "information integrity" across contexts. "Attributes" refer to "accuracy, consistency, and reliability", which are the most commonly associated components of the term in existing literature.

OECD, 2024; GAC, 2023; Adam et al., 2023). For example, in the information environment, the system (e.g., national information ecosystem) includes humans, the tools they use to process and share information, the information as shareable outputs, and the relationships between these three things. While it may be reasonable or even desirable to assess the degree of accuracy, reliability, and consistency of information on a specific topic within an information ecosystem to ensure citizens' ability to make informed decisions, it may not be reasonable to do so regarding the flow of that information between people and communities, given privacy and human rights concerns. Following this logic, attributes related to 'trust' have less to do with the quality of information so much as the response that information receives among human audiences, which cannot be measured in assessing the information itself but in studying perception or cognition. For the sake of conceptual goodness, future definitions of "information integrity" should differentiate between the integrity of information and the integrity of the system or methods by which it is processed, shared, and consumed. While the two are inextricably linked, one refers to the state of information, while the other refers to the processes through which information is changed and exchanged. In other words, they deal with different concepts.

For attributes to be coherent, they also need to tie into the same goal. Following definitions provided by information security, accuracy, consistency, and reliability are critical attributes of information integrity. That is because they all contribute toward the defined goal of information integrity, which is to maintain the quality of information in a closed system. In the context of the information environment, an oft-identified purpose of information integrity is to enable citizens to make informed decisions, including political choices, but also in responding to crises, such as natural disasters and pandemics. There needs to be more clarity in existing definitions on how identified attributes can contribute to that aim.

### *4.5 Differentiation: How Differentiated Are the Instances and the Attributes (from Other Most-Similar Concepts)?*

There appears to be no other term like "information integrity" used to describe the ideal state or quality of information societies might want in the information environment. The closest term to it is "data integrity", which scholars have argued is conceptually distinct from "information integrity" (Boritz, 2005). However, the insufficient articulation of what is meant by "information integrity", beyond the listing of suggested attributes, makes differentiation difficult.

Based on our analysis, multilateral organizations adopted the term information integrity to expand beyond combatting disinformation, which is a narrow, threat-based focus that has become heavily politicized. More will need to be done to differentiate the two ideas. Indeed, one of the biggest risks for "information integrity" is that it simply becomes synonymous with disinformation. For example, the Council of Europe's Working Group on the Integrity of Online Information

produced a guidance note and explanatory memorandum on their work (MSI-INF, 2023a, 2023b). The guidance notes provided detailed definitions for disinformation, misinformation, and 13 related terms [1–2]. It did not, however, define "information integrity" and only mentioned "integrity" once in the context of elections. (MSI-INF, 2023a) The rest of the document repeatedly refers to "mis/disinformation," leaving the reader to infer that lack of integrity and disinformation might be synonymous. The explanatory memorandum mentioned "fact-checking" [4] and "resilience against mis-and disinformation" [15] as components of information integrity. The document could have benefitted from a clearer definition of "information integrity" itself and how it differed from efforts to combat mis- and disinformation and to improve reliable sources of information. The conflation between information integrity and disinformation also occurs in how initiatives purporting to be framed around the former are positioned. For example, one of the outputs from the Summit for Democracy Cohort on Information Integrity was to develop an "Information Integrity Organization Map and Resources." Not only did this map mirror the same types of initiatives that others had tracked on disinformation (Smith, 2020), in all four types of initiatives listed (e.g., fact-checking, media literacy and training organizations, research and monitoring, and policy and standards organization) the sole common denominator was related to countering "misinformation and disinformation" (ASD, n.d.). This conflation between information integrity and disinformation renders the newer term susceptible to politicization by actors that are unsupportive of related efforts.

We believe that information integrity offers an opportunity for democracies to construct a more systemic framework for maintaining healthy information ecosystems, above and beyond a narrow focus on risks posed by disinformation. However, that must be demonstrated both through how the concept is defined and how its attributes are enabled through policy and practical initiatives. The original definition of "information integrity" includes more attributes than the accuracy of information. However, if policymakers focus on that attribute in excess, advocating for value-based concepts like truth, they risk conflating information integrity with disinformation (Samonas & Coss, 2014; Seadle, 2018; Rügenhagen et al., 2020). One approach to avoid this pitfall would be to ask what the goal of pursuing information integrity is before adopting it as a term, and if there is an intention to go beyond countering disinformation and assess the state of the information environment at large.

### *4.6 Depth: How Many Accompanying Properties Are Shared by the Instances Under Definition?*

Achieving Gerring's idea of conceptual goodness is no simple feat. It requires meeting a balance between ease of communication and definitional depth. Where parsimony demands a term be succinct in its use of attributes, depth suggests that the

greater number of attributes that uniquely comprise a definition enhances its conceptual goodness. In this sense, "a concept is enhanced by its ability to 'bundle' characteristics" [380]. In other words, it isn't a matter of how many attributes are included but rather how those attributes collectively make a concept rich and unique. Here, "information integrity" is challenged in that most definitions of the concept lack an explanation for what the accompanying attributes (and objectives aimed to be achieved by using it) mean. As it stands, many definitions of "information integrity" are a list of their component parts alone, which often do not correlate as argued earlier. Less than a quarter (20%) of definitions reviewed here offered definitions of the attributes used in the concept of information integrity. Of particular concern are those texts that propose using information integrity in relation to information environments in democracies given apparent repercussions for policy-making. This can easily be rectified by defining each of the attributes and articulating how it relates to contributing to and/or maintaining information integrity in the context of an information environment through corresponding activities. As it stands, information integrity needs more depth as a concept.

## *4.7 Theoretical Utility: How Bounded, How Operationalizable, Is the Concept?*

For a concept to have theoretical utility, according to Gerring, it must "aid in the formulation of theories." In this way, "concepts are the building blocks of all theoretical structures, and the formation of many concepts is legitimately theory-driven," which creates a need for classificatory frameworks. For this to be the case with information integrity, consistent definitions of it would be required, starting with the use of attributes and sufficient articulation of how each of these may inform associated policy or practical initiatives. As it stands, even in the field from which it emerged—information security—information integrity will be challenged as a foundation with so many variations on its meaning.

## *4.8 Field Utility: How Useful Is the Concept Within a Wider Field of Inferences? How Useful Is the Concept Within a Field of Related Instances and Attributes?*

In order to retain conceptual goodness and be practically useful across various applied fields, including in addressing some of the information environment threats discussed here, the definition of information integrity must be transferable. As we have seen with analyzed uses of "information integrity" by multilateral initiatives, which are ostensibly aiming to address identified threats or other practical purposes, the original meaning from information security is often lost or greatly diluted. This

is so not just in the use of attributes but also in how they are applied to information, the overall information ecosystem or in desired outcomes. As an increasing number of policy and practical streams across governments, industry and civil society demand greater consilience and coordination on information/digital issues a lack of clarity in definitions will make it harder to develop consistent concepts for proactive and practical implementation.

Take for example, the existing lack of clarity on the roles of government in upholding information integrity. While existing literature implicitly assumes that governments should play a key role, this may not be an applicable model in countries with recent histories of, or current backsliding into, authoritarianism. Questioning these assumptions can help remove barriers to understanding the concept in a more global context and support its operationalization (Santos, 2024).

## 5 Conclusion and a Way Forward

Does information integrity have conceptual goodness? In our assessment, not yet, but it could. "Information integrity" is familiar to some audiences, but that needs to be further explained, and in so doing, it will acquire further clarity. As it stands, "information integrity" is increasingly used in policy circles beyond its origins in information security, but as such it is often treated like the concept is already assumed to be widely understood or fixed (Santos, 2024). As this chapter has shown, the concept of information integrity is far from fixed or universal, not just across stakeholders using it, but often even in a single field. This consistency is required to ensure that information integrity resonates with the same sense and meaning when it does become a more familiar term. To that end, as a concept, information integrity should be limited to focus first on the attributes associated with the integrity of information, drawing from its original definition, separating out concepts related to processing information or the system, as well as desired outcomes in pursuing information integrity. These three concepts—information integrity, the integrity of the information environment, and desired outcomes—can and should be discussed in tandem, but definitions of each are best not done in one sentence. Greater clarity in what constitutes "information integrity", namely its component parts, will also help distinguish it from other concepts like disinformation. All of the above needs to be achieved before information integrity can ultimately have both theoretical and field utility. As it stands, information integrity lacks conceptual goodness, but it has the potential to achieve it if given a proper and consistent definition, which is adopted and used by a variety of stakeholders.

Before we define "information integrity," it might be worthwhile to lay out why we care about the concept and what we hope it will achieve. Indeed, a strategic vision is necessary to ensure that all the stakeholders share the same aims and direction. Working backward, a strategy helps envision the information environment we hope to see in pursuing information integrity and should inform what guidelines and

principles are necessary for pursuing that. From there, additional attributes might follow.

Moreover, information integrity pertains only to information within the information environment. The larger information environment, however, contains processes that impact said integrity, such as the means through which people access or produce information. A better understanding of the whole system can support the development of attributes of information integrity that would be important in achieving those aims. This could begin with an exercise to map out current information ecosystems—the way information is produced, consumed, disseminated, and governed in them—and find vulnerabilities and pain points.

**With a better understanding of the whole system and what might be needed to secure it, we can turn to the attributes of information integrity that would be important in achieving those aims. Choosing a concise set of attributes, clearly defining them, and laying out ways to measure and assess them would be the next steps. Any attempt at defining "information integrity" in the context of democracies should involve a multistakeholder approach to achieve consensus. In this, the people should not be forgotten. The state of the information environment strongly affects citizens within it. There are ways to incorporate the public's perspective in the defining of "information integrity," such as citizen assemblies (Farrell & Suiter, 2021). This will be increasingly necessary in a polarized world with declining rates of trust that will impede information integrity measures. We can have the best definitions and policies built around them in the world, but they will be pointless if people do not trust them.****AcknowledgmentsThe authors are grateful to Michael Berk for his feedback on the article.**

**Competing Interests** The authors are affiliated with the Carnegie Endowment for International Peace's Information Environment Project. The IEP is grateful for funding provided by the Government of Canada, the William and Flora Hewlett Foundation, Craig Newmark Philanthropies, the John S. and James L. Knight Foundation, Microsoft, Meta, Google, Twitter, and WhatsApp. The IEP is wholly and solely responsible for the content of its products, written or otherwise. We welcome conversations with new donors. All donations are subject to Carnegie's donor policy review. We do not allow donors prior approval of drafts, influence on selection of project participants, or any influence over the findings and recommendations of work they may support.

## References

Adam, I., Lai, S., Nelson, A., Wanless, A., & Yadav, K. (2023). Emergency management and information integrity: A framework for crisis response. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2023/11/09/emergency-management-and-information-integrity-framework-for-crisis-response-pub-90959.

Alliance for Securing Democracy. (2023). The summit for democracy cohort on information integrity. German Marshall Fund. https://securingdemocracy.gmfus.org/wp-content/uploads/2023/10/The-Summit-for-Democracy-Cohort-on-Information-Integrity-.pdf.

Alliance for Securing Democracy (n.d.). Information integrity organization maps and resources. German Marshall Fund. https://web.archive.org/web/20231208235722/https://securingdemocracy.gmfus.org/information-integrity-map/.

Becker, H. B. (1983). *Information integrity: A structure for its definition and management*. McGraw-Hill.

Blinken, A. J. (2024). *Building a more resilient information environment* [Speech transcript]. U.S. Department of State. https://www.state.gov/building-a-more-resilient-information-environment/.

Boritz, J. E. (2005). IS practitioners' views on core concepts of information integrity. *International Journal of Accounting Information Systems, 6*(4), 260–279. https://doi.org/10.1016/j.accinf.2005.07.001

Boritz, J. E., & Datardina, M. (2019). A framework for information integrity controls. Chartered Professional Accountants, Canada. https://www.cpacanada.ca/-/media/site/operational/rg-research-guidance-and-support/docs/02049-rg-framework-information-integrity-controls-april-2019.pdf.

Bovee, M., Srivastava, R. P., & Mak, B. (2003). A conceptual framework and belief-function approach to assessing overall information quality. *International Journal of Intelligent Systems, 18*(1), 51–74. https://doi.org/10.1002/int.10074

Date, C. J. (1997). *An introduction to database systems*. Pearson Education India.

DeLone, W. H., & McLean, E. R. (1992). Information systems success: The quest for the dependent variable. *Information Systems Research, 3*(1), 60–95.

Farrell, D. M., & Suiter, J. (2021). *Reimagining democracy: Lessons in deliberative democracy from the Irish front line*. Cornell University Press.

Flowerday, S., & Von Solms, R. (2005). Real-time information integrity= system integrity+ data integrity+ continuous assurances. *Computers & Security, 24*(8), 604–613.

Fu, H., McLeod, P., Cockerill, P., Hammer, C., Hiraga, M., & Gomez, M. G. T. (2022). Decades of learning and experience from the trust fund for statistical capacity building to inform the new global data facility. World Bank. https://blogs.worldbank.org/en/opendata/decades-learning-and-experience-trust-fund-statistical-capacity-building-inform-new-global.

Geisler, E., Prabhaker, P., & Nayar, M. (2003). Information integrity: An emerging field and the state of knowledge. In *PICMET'03: Portland international conference on management of engineering and technology management for reshaping the world* (pp. 217–221). IEEE.

Gerring, J. (1999). What makes a concept good? A critical framework for understanding concept formation in the social sciences. *Polity, 31*(1), 357–393.

Global Affairs Canada. (2023) *Global declaration on information integrity online*. Retrieved April 4, 2024, from https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/declaration_information_integrity-integrite.aspx?lang=eng.

Grabe, M. E., & Bucy, E. P. (2022). Moral panics about the integrity of information in democratic systems: Comparing tabloid news to disinformation. *Journal of Broadcasting & Electronic Media, 66*(4), 565–591.

Harley, K., & Cooper, R. (2021). Information integrity: Are we there yet? *ACM Computing Surveys (CSUR), 54*(2), 1–35.

Khan, I. (2021). Disinformation and freedom of opinion and expression: Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression. United Nations Human Rights Council Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. https://digitallibrary.un.org/record/3925306?ln=en&v=pdf.

Khan, Q., Butt, M. A., Zaman, M., & Asger, M. (2013). A novel approach based information integrity modeling. *International Journal of Engineering Science and Innovative Technology (IJESIT), 2*(1), 210–215. https://www.ijesit.com/Volume%202/Issue%201/IJESIT201301_31.pdf.

Mandke V. V. (1996). Research in information integrity: A survey and analysis. Proceedings of the JNCASR and SERC discussion meeting at IISc campus, Bangalore on information integrity—issues and approaches (ed. Rajaraman V. & Mandke V.V.), Information Integrity Foundation. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=1c59cdc7a7229907932a880a28f0231ccf64e22e.

Matasick, C., Villanova, N., & Zdanavicius, L. (2024). Facts not fakes: Tackling disinformation, strengthening information integrity. organisation for economic co-operation and development. https://doi.org/10.1787/d909ff7a-en

MSI-INF. (2022). Meeting report: Committee of Experts on the Integrity of Online Information. Council of Europe. Retrieved March 26, 2024, from https://www.coe.int/en/web/freedom-expression/msi-inf.

MSI-INF. (2023a). Guidance note on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner. Council of Europe. Retrieved March 26, 2024, from https://rm.coe.int/cdmsi-2023-015-msi-inf-guidance-note/1680add25e.

MSI-INF. (2023b). Explanatory memorandum to the guidance note on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner. Council of Europe. https://rm.coe.int/cdmsi-2023-16-msi-inf-explanatory-memorandum/1680add260.

Napoli, P. M. (2025). In pursuit of ignorance: The institutional assault on disinformation and hate speech research. *The Information Society: An International Journal, 41*(1), 1–17.

Nayar, M. K. (2002). The information integrity imperative. In M. Gertz, E. Guldentops, & L. Strous (Eds.), *Integrity, internal control and security in information systems* (pp. 187–193). Springer US. https://doi.org/10.1007/978-0-387-35583-2_11

Nayar, M. K. (2007). Information integrity (I*I): The next quality frontier. *Total Quality Management & Business Excellence, 15*(5–6), 743–751. https://doi.org/10.1080/14783360410001680224

Organisation for Economic Co-operation and Development. (n.d.-a). *The OECD dis/mis resource hub.* Retrieved March 26, 2024, from https://www.oecd.org/stories/dis-misinformation-hub/

Organisation for Economic Co-operation and Development. (n.d.-b). *OECD Expert group on governance responses to mis- and disinformation.* Retrieved March 26, 2024, from https://www.oecd.org/gov/oecd-expert-group-on-mis-and-disinformation/

Rügenhagen, M., Beck, T. S., & Sartorius, E. J. (2020). Information integrity in the era of fake news: An experiment using library guidelines to judge information integrity. *Bibliothek Forschung und Praxis, 44*(1), 34–53. https://www.degruyter.com. https://doi.org/10.1515/bfp-2020-0005/html

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security, 10*(3).

Santos, N. (2024). *Why do we need to discuss so-called 'Information Integrity'?* Tech Policy Press. https://www.techpolicy.press/why-do-we-need-to-discuss-socalled-information-integrity/.

Seadle, M. (2018). An introduction to the column. Humboldt-Elsevier Advanced Data & Text Centre. Retrieved March 26, 2024, from https://web.archive.org/web/20230321043105/https://headt.eu/An-Introduction-to-the-Column/.

Shaker, L. (2006). In Google we trust: Information integrity in the digital age. *First Monday, 11*(4). https://doi.org/10.5210/fm.v11i4.1320

Smith, V. (2020). Mapping worldwide initiatives to counter influence operations. Carnegie Endowment for International Peace. https://carnegieendowment.org/2020/12/14/mapping-worldwide-initiatives-to-counter-influence-operations-pub-83435.

Sinnett, W. M. (2008). Excellence in information integrity. Financial Executives Research Foundation.

Trites, G. (2013). Information integrity. AICPA Assurance Services Executive Committee's Trust Information Integrity Task Force and the Canadian Institute of Chartered Accountants. https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/asec-information-integrity-white-paper.pdf.

United Nations. (2023). Our common agenda policy brief 8: Information integrity on digital platforms. https://www.undp.org/policy-centre/oslo/publications/strategic-guidance-information-integrity-forging-pathway-truth-resilience-and-trust.

United Nations. (2024). United Nations global principles for information integrity: Recommendations for multi-stakeholder action. https://www.un.org/sites/un2.un.org/files/un-global-principles-for-information-integrity-en.pdf.

United Nations Development Programme. (2022). Strategic guidance: Information integrity: Forging a pathway to truth, Resilience and Trust. United Nations Development Programme. https://www.undp.org/policy-centre/oslo/publications/strategic-guidance-information-integrity-forging-pathway-truth-resilience-and-trust.

United Nations Development Programme. (2023). *UNDP iVerify: A monitoring and evaluation framework*. https://www.undp.org/policy-centre/oslo/publications/undp-iverify-monitoring-and-evaluation-framework.

United Nations General Assembly. (2021). Countering disinformation and promotion and protection of human rights and fundamental freedoms: Resolution / adopted by the General Assembly A/RES/76/227. https://digitallibrary.un.org/record/3955093?ln=en.

Wanless, A., Lai, S., & Hicks, J. (2025) Assessing national information ecosystems. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2025/02/assessing-national-information-ecosystems?lang=en.

World Leadership Alliance-Club de Madrid. (2018). Protecting information integrity: National and International Policy Options: Report of the roundtable on global governance for information integrity held in Riga (Latvia) on 27 September 2018. https://clubmadrid.org/wp-content/uploads/2019/03/Protecting-Information-Integrity-WEB.pdf.