Internews | acaps

Technical brief
May 2023

INFORMATION LANDSCAPE DATASET

Methodology guidance on the analysis and information events and trends in humanitarian settings

TABLE OF CONTENTS

INTRODUCTION

This technical brief forms part of a joint work between ACAPS and Internews. It accompanies the publication of the ACAPS Information Landscape Dataset and gives guidance on the analysis of the information landscape (or 'information ecosystem') in humanitarian settings, the events and trends that affect the lives of people in crisis, and the humanitarian organisations operating at global and subnational levels. It does so by incorporating information indicators into relevant ACAPS analysis products. The methodology assesses information access, contexts, content providers, and gaps relevant to humanitarian crisis situations and responses.

The analysis of the global-level information landscape, events, and trends in humanitarian settings integrates with ACAPS' broader global crisis analysis by summarising the information ecosystem in countries with occurring or emerging humanitarian crises. Organisations can adapt the information indicator analysis to the subnational level to contribute to country-level analyses and products and inform humanitarian organisations' analysis and decision-making around access constraints, community needs, and factors relevant to community engagement and accountability.

The information indicator and analysis methodology informs analysis by collating qualitative information sources and datasets structured across the four indicators. It carries limitations associated with the information used, as described in more detail in the Limitations section of this document.

ABOUT THIS TECHNICAL BRIEF

This guide was written by Emily Cowlrick, Stijn Aelbers, and Masud Rana (Internews) and Marwa Alsubeih and Claudia Manili (ACAPS). The development of this technical brief was generously supported by the Cisco Foundation.

DEFINITIONS

DATA CATEGORIES

These are flagged as "Type" in the dataset.

Context: the underlying conditions that affect the ability of people, groups, and institutions to seek, create, and share information. These conditions can involve communication infrastructure, geography, language, socioeconomic conditions, culture, gender, literacy, legality, and vulnerability.

Information trend: a series of events that indicate a change in information-seeking behaviour or emerging or recurrent interest in certain topics in a specific time frame.

Information event: an event that affects the way people can access, share, or produce information, with a focus on those that can cause harm or worsen the capacity of people in crisis to keep themselves safe or improve their situation.

GENERAL DEFINITIONS

Information access: the capacity and opportunity for people in crisis to access information. Physical circumstances, sociocultural barriers, and interventions from authorities or institutions may hamper access. The unintended consequences of these interventions, such as internet shutdowns, phone ownership, and damaged infrastructure, might also hamper access.

Information content: topics and themes circulating among people in crisis, potentially causing harm or confusion, or generating discussions that could further polarisation and ultimately conflict between individuals or particular groups.

Information gaps: unaddressed information needs among people in crisis resulting from a lack of understanding of people's needs and sociocultural taboos, a lack of capacity to fill the gap (like language skills), or particular gaps in the available information as a result of deliberate interventions (like censorship or self-censorship).

Information providers: individuals, groups, and institutions that select and share information. Information providers are relevant to information landscapes, trends, and events, as they can have an impact on people's decision-making – whether positive or negative, deliberate or involuntary. Creating content that is harmful to certain individuals or groups or excluding or censuring certain content can achieve this impact. Harm can also come from blocking channels or providing channels or platforms for information that present risks for people in crisis. Information providers can be sources or channels (as below); it is important to note the distinction between them.

Information source: an information source is a person or institution from which information originates. Primary or secondary data can form information sources. In a humanitarian crisis, important sources are humanitarian organisations, governments, local media, and community members, whether online or offline. These sources can pass on information without necessarily verifying it. Passing on information, instead of creating it, essentially makes them a 'channel' instead of a 'source', even when people might refer to them as such.

Information channel: the means used to exchange information, whether face-to-face, TV, radio, print, or online. With traditional media, the source and the channel are often seen as one and the same: the radio station broadcasts using FM channels, TV stations use TV channels, etc. In the past, (a limited amount of) private or public media had the capacity to create and disseminate content; at present, these few providers would disseminate content through (online) channels that they shared with individuals and media outlets worldwide. This shift has made it more important to differentiate between the channel ('social media') and the source (a reputable news outlet, the government, or hearsay).

Social media platform: online services that provide an environment for the exchange of information without the need to create content. These platforms can include, but are not limited to, YouTube, Facebook, Twitter, NextDoor, LinkedIn, Instagram, Google, and Reddit. Messaging apps, such as Facebook Messenger, WeChat, WhatsApp, Signal, Viber, and Telegram, are often referred to as part of social media. While the focus of these platforms is to connect people, other users also include governments, businesses, news media, and the entertainment industry, making it hard to distinguish between individually created content and professionally created (and verified) information.

METHODOLOGY

Framework

The Information Event Analysis Framework is a stand-alone framework that can be integrated into any relevant ACAPS framework, thereby enabling its inclusion in analysis and analysis products. The framework description below outlines the framework as a stand-alone product.

This Information Event Analysis Framework is based is based on 4 indicators and 14 sub-indicators:

INFORMATION TRENDS	ACCESS TO INFORMATION	VULNERABILITY OF SPECIFIC GROUPS WITHIN THE CONTEXT / SAFETY AND DIGNITY OF PEOPLE ACCESSING INFORMATION	INFORMATION FREEDOM AND SECURITY
Disinformation trends	Telecommunication infrastructures damage or limitations	Stigma trends	Journalist safety
Misinformation trends	Accessible, safe and accurate information	Hate-speech trends	Censorship and self-censorship
Malinformation trends	Trust in information		Digital Security
	Information literacy		Deliberate communication shutdowns / restrictions from malicious actors
	Digital literacy		

Source: ACAPS

INTERCHANGEABILITY OF ACAPS' FRAMEWORK AND DATASETS

This dataset directly informs different ACAPS products, such as the Humanitarian Access Overview (see subindicators 2.1 and 4.3). Generally, users should use it with other access datasets, such as the INFORM Severity Index, the Protection Indicators Monitoring dataset, the Humanitarian Access Events Monitoring dataset, and the Seasonal Calendar, for a holistic understanding of the landscape of continuing crises.

DESCRIPTION OF INDICATORS AND SUBINDICATORS

Information trends

Disinformation trends

Disinformation refers to false information that providers deliberately spread to mislead or deceive others. Disseminating disinformation is the act of knowingly and purposefully spreading misinformation. Examples of disinformation include propaganda, 'counterfeit' news (such as websites and social media accounts impersonating a well-known brand or person), conspiracy theories, and pseudoscientific reports developed to deliberately share false or misleading information.

Disinformation trends can refer to increased or changed instances of disinformation, either generally or on a particular theme (for example, health-related or about a particular group). Increased disinformation trends against particular populations can aggravate conflict, hate speech, and, in some cases, real-world harm and atrocities against people. Monitoring under this subindicator can identify disinformation trends in information content and information providers.

Trend example: in Myanmar, the Government flooded social media with fake accounts and invented stories as part of a deliberate effort that eventually included real-world violence and genocide against the Rohingya.

Event example: in one particular instance, the government widely posted a fake story about a Muslim man raping a Buddhist woman.

Misinformation trends

Misinformation refers to any false or inaccurate information that is spread or communicated in any form, regardless of whether or not it is meant to mislead or deceive others. Misinformation as a practice is a typical and inevitable part of information-sharing between people. Examples or alternative terms for misinformation can include false rumours, gossip, and exaggerated realities to entertain others.

Not all instances of misinformation are relevant to the misinformation trends indicator. Relevant trends to analyse include increased instances of misinformation in contexts where that misinformation could cause real-world harm. Examples include misinformation around health advice, access to humanitarian aid or services, or the movement or status of refugees or displaced people. Changes or increases in misinformation for a particular group or community are also worth noting, as this may indicate breakdowns in sources those groups trust and find reliable, making communication difficult to navigate and causing harm in the future. Groups of concern include vulnerable or marginalised groups, such as people with disabilities, women, or people with diverse sexual orientation, gender identity and expression, or sex characteristics (SOGIESC). Monitoring under this subindicator can identify misinformation trends in information content and information providers.

Event example: the Russian invasion of Ukraine pushed COVID-19 from the front of the news cycle, resulting in a deprioritisation of information about the virus.

Trend example: when Russia invaded Ukraine, those working on the pandemic response noticed increased rumours that COVID-19 was a hoax. The war in Ukraine had taken over the news, resulting in less coverage of the COVID-19 pandemic. This coverage gap meant information circulated that the pandemic was over or was not a real problem. Mentions of COVID-19 being a hoax also increased at this time.

Malinformation trends

Malinformation is factual information that is misappropriated or used to inflict harm, either through negligence or active harm. It can refer to information that stems from facts but that people exaggerate, frame, or alter to be intentionally misleading.

Event example: a popular national newspaper published a front-page story that included the names, pictures, and locations of people suspected of being gay in a country where being so was illegal. In this case, the newspaper shared the story to vilify and endanger those gay people.

Access to information

Telecommunication infrastructure damage or limitations

This indicator refers to damage to or the changed functioning of telecommunication infrastructure, including disrupted phone or internet networks (physical infrastructure), electricity outages, or damage to other physical infrastructure that networks rely on. Such physical infrastructure can include buildings, data centres, or bridges. Damage can include intentional damage (for example, in war or conflict situations) or unintentional damage (for example, in natural disaster situations).

Event example: an earthquake damaged all communication infrastructure. Mobile phone operators quickly restored their network, but FM towers and repeaters remained down, and local radio stations suffered damage and stopped broadcasting.

Context example: the media landscape in the affected country is very political.

Trend example: as a result of the context, humanitarian organisations were reluctant to get involved in rehabilitating the local radio network.

Accessible, safe, and accurate information

This subindicator captures constraints in accessing information. An accessible channel involves the timeliness of information, the availability of information in relevant languages, access to accurate information, and access via trusted and safe sources. Monitoring should capture changes in people's access to this type of information. A change in access might result from the movement of people, general information access restrictions and sharing during conflict or natural disasters, or authorities targeting restrictions on rights-based information.

Event example: the Government of Türkiye blocked Twitter following increased criticism about the Government's earthquake response.

Trend example: Syrian refugees would sell their mobile phones to pay for boat rides across the Mediterranean and have less access to information upon arrival.

Trend example: the authorities do not allow Rohingya refugees in Bangladesh to purchase sim cards until after their registration, which typically takes years, resulting in limited access to information.

Trend example: people crossing borders are not provided with information about their right to seek asylum in their language.

Trend example: because of international stigma, a certain government does not allow the distribution of any information about cholera and instead imposes the term 'watery diarrhoea', making communication less effective.

Trust in information

Trust is a fundamental factor in accessing information. Whether someone trusts an information source guides if they will listen to, act on, and share the information gained from that source. A lack of trust usually leads individuals and communities to not engage with a certain information source, and blind trust can result in lower levels of agency and a higher risk of mis-, dis-, and malinformation. Organisations and initiatives that track trust trends at the group and community levels inform this subindicator. Internews incorporates trust in their Information Ecosystem Assessments and community data monitoring (including 'rumour tracking').

Trend example: community perception monitoring in the Ebola response indicates that many people do not trust the intentions of humanitarians because they do not know or understand any specifics about it, and because the community is not part of the decision-making about the response. When asked if they believe the information coming from humanitarian organisations about the Ebola virus, most say they do not and point to corruption accusations among the responding organisations.

Context example: there are high levels of mistrust resulting from corruption in international humanitarian organisations.

Event example: an interview with two French doctors on vaccine testing – where they talked about testing first on African people – sparked fury across the African continent.

Information literacy

Information literacy refers to the ability and capacity to find, evaluate, organise, use, and communicate information (in various formats), media content, and sources for accuracy, reliability, and evidence of bias. A lack of or lower levels of information literacy increase the risk for people in situations requiring decision-making, problem-solving, or knowledge acquisition. Assessments of information literacy often occur via Internews' Information Ecosystem Assessments.

Context example: a report shows that young people between the ages of 15–30 in the Philippines are more likely to check the source of information, compare content with other trusted sources, and validate information with trusted information providers – in contrast to people over 60, who are more likely to share misinformation and less likely to check the source before sharing.

Digital literacy

Digital literacy refers to the ability and capacity to safely, effectively, and responsibly use, comprehend, manage, and analyse technology, digital tools, and channels. Technological literacy can be applied to the internet, smartphones, computers, tablets, applications, software, and social media platforms, among other things. In the context of information events, technological literacy most notably applies to that which supports the acquisition or sharing of information to support decision-making, problem-solving, and knowledge-building. Assessments of digital literacy often occur via Internews' Information Ecosystem Assessments.

Trend example: a recent survey of a refugee population indicates that many rely on location-sharing on their phones to inform their families back home of their location. The survey shows very little awareness of the risks associated with location-sharing, including how it can allow border control and other authorities to follow people's movements.

Vulnerability of specific groups within the context / safety and dignity of people accessing information

Stigma trends

Stigma refers to the devaluing or discrediting of an individual or group based on their personal characteristics or attributes – for example, their mental health condition, migrant status, diverse SOGIESC, or socioeconomic status. Stigma trends as an information event subindicator refer to trends in how information content or providers drive stigma in communities, whether online or offline. A significant event would be when an increase in the sharing of stigmatised information results in real-world harm (e.g. making

people feel that they need to hide factors about themselves for their safety). Also included are stigma trends may change or decrease information access for particular people.

Trend example: a chickenpox outbreak circulates within Community X, and information indicates it is more prevalent among gay people. The outbreak is connected with an increase in anti-LGBTQ+ sentiment online, in messaging apps, and in local media. Health services become concerned with the general stigma around gay people, and the known prevalence of chickenpox within that population reduces the LGBTQ+ community's uptake of other services.

Event example: the Venezuelan partner of a pregnant woman in Ecuador stabs and kills her, resulting in increased stigma towards Venezuelan migrants in online environments.

Hate speech trends

Hate speech is defined as offensive discourse (communication in speech, writing, or behaviour) that attacks or uses pejorative or discriminatory language about a person or group based on their inherent personal characteristics, such as religion, ethnicity, nationality, migrant status, gender, or diverse SOGIESC. Hate speech trends as an information event subindicator refers to trends in how information content or providers contribute to or drive online or offline hate speech, whether intentionally or unintentionally. A significant event would be when the increased sharing of hate speech results in real-world harm (e.g. causing attacks on a particular group).

Event example: the US President refers to migrants crossing the border as "animals, criminals, and rapists". In the wake of these comments, derogatory social media posts about migrants, particularly calls to violence against migrants, significantly increase. More and more instances of harassment and attacks towards refugees are also reported.

Information freedom and security

Journalist safety

This subindicator refers to changed or increased instances of compromises or threats to journalists' physical or psychological safety. Threats can include harassment, imprisonment, and those directed by entities with malicious intentions or the public towards family members or associates of the journalist being attacked. Threats can also include unsafe environments, such as volatile post-disaster conditions or conflict situations, where threats are not specifically directed towards journalists but they are nonetheless at risk. This subindicator points to changes in the information context or to the underlying causes and circumstances that make information events more likely to occur or that worsen their impact on people in crisis.

Event example: the public harasses radio reporters working on the Ebola outbreak in the streets and kills two journalists in the Democratic Republic of Congo.

Trend example: the aggression towards journalists is related to widespread distrust around the humanitarian response to Ebola, with the public seeing local media as a 'mouthpiece' for foreign NGOs.

Censorship and self-censorship

Censorship refers to the suppression or prohibition of information content and providers. Reasons for censorship can include obscenity, political unacceptability, and security threats. Governments and alternative authorities, media outlets, institutions, and individuals can undertake and enforce censorship. Censorship can occur online or offline, affecting the media and all forms of information-sharing.

Self-censorship refers to the act of censoring or classifying one's own discourse. This act is done out of fear of, or deference to, the sensibilities or preferences (whether actual or perceived) of others and without overt pressure from any specific party or institution of authority.

In the context of information events in humanitarian crises, the most relevant form of censorship and self-censorship for monitoring and analysis is that which results from the actions of entities with malicious intentions.

Trend example: following the 2021 Taliban takeover of Afghanistan, many journalists, media outlets, and influencers have self-censored the content they produce and share out of fear of reprisal from Taliban authorities. This fear is based on threats and attacks that other journalists or people of influence have experienced instead of an explicit declaration from Taliban authorities on what information is acceptable.

Digital security

Digital security refers to resources and standards that protect individuals' online identities, data, and other assets. Individuals can undertake digital security processes depending on how they agree to manage and share their data or online identity, as can institutions and organisations that control the data or spaces that process and use data. As relevant to humanitarian contexts and crisis-tracking, this subindicator typically refers to situations or entities that put a particular group's digital security under threat, either intentionally or unintentionally.

Event example: an authoritarian regime set up a mock website through which people could volunteer with food distribution programmes. The regime denies the humanitarian crisis in their country, meaning they consider all the people who signed up as 'opposition', including those working for or collaborating with INGOs.

Deliberate communication shutdowns / restrictions from malicious actors

This subindicator refers to entities with malicious intentions who deliberately enforce communication shutdowns or information access restrictions, including internet shutdowns for particular populations, restrictions on certain websites, and the shutdown of or threats to particular media houses or media types (for example, independent media). While these events also inform levels of information access (Indicator 2), this subindicator analyses shutdowns and restrictive events that inform changing levels of information freedom and security within the information context.

Trend example: refugees who have just crossed the border have no right to buy a sim card before they are fully registered. The registration process takes a long time, and some people are avoiding registration as they are trying to move on to the next country. As a result, many people look for loopholes, such as through local vendors selling sim cards and fake personal details, to still be able to access online information sources.

SOURCES

This framework seeks to guide data collection from the most reliable and relevant sources at any given time in a specific context. The table below provides an example of some data sources that can inform the information event indicators. The maintenance and adaption of a full annex of sources (see the example in Annex 1) will be according to the following structure:

TYPE OF DATA SOURCE	SUBNATIONAL OR GLOBAL ANALYSIS	LIKELY UPDATE FREQUENCY	RELIABILITY	RELEVANCE TO FRAMEWORK
Primary data sources Primary data sources include community-level data, such as feedback mechanisms, Internews' misinformation management programme, and rumour-tracking projects. The availability of this data usually depends on the activities undertaken in a country, as they focus on a particular humanitarian event or context and a particular population or target group. This data usually feeds into a subnational analysis only and is context-specific.	Subnational	Less frequent, depends on the activities in the country	Community data, not individually verified	Highly relevant and provides context-specific information on emerging trends
Secondary data sources Secondary data sources include information from organisational, agency, and cluster assessments relevant to the information event indicators. This information can include past assessments that inform the analysis of the information context, but preferably sources that are updated based on particular humanitarian crisis contexts.	Subnational and global	Frequent, from a range of sources	Reliable, verified sources only	Generalised and non-context-specific risks

LIMITATIONS

ACAPS aims to monitor and track information event indicators daily at the global and subnational levels. The intended coverage of the dataset is focused on the countries where, according to ACAPS methodologies, there is an active humanitarian crisis. This dataset presents a broad coverage of the reported information to flag events and trends that may affect the information ecosystem. The goal is to inform operational, strategic, and policy decision makers about information access constraints, community information needs, and factors relevant to community engagement and accountability. The diversity and complexity of different crises mean that certain events may appear to fall outside the categorisation of indicators. Data might not be complete because of the high volatility of some crises, and there may be delays in recording certain events and trends. Secondary data sources are sometimes outdated, with no exact information about the events' dates. ACAPS relies on open sources and the expert judgement of trained data collectors in selecting the most reliable sources and does not have an operational presence in every country; for this reason, some events may not be recorded.

Organisations may use official statistics or researchers' findings that use indicator methodology measurements relevant to changing time-sensitive information or differently defined or categorised variables. Information may also be published without a clear indication of where it happened, in effect lacking clarity and representativeness. Another major disadvantage to using open sources is that data collectors do not know exactly how the data collection processes and analyses were done. Finally, linguistic barriers may prevent ACAPS from identifying all the available information. When ambiguous or conflicting data is found, we hold an analytical discussion to reach a common agreement on coding.

ACAPS integrates some of Internews' collected and harmonised primary data with the presented ACAPS framework.

DATA STRUCTURE

COLUMN NAME	DATA TYPE	CONTENT
ID	Number	Number
ISO	String	ISO3 country identifier
Country name	String	Name of the country
Countrywide	Boolean	Geoscope – yes/no
ADMIN1	String	Geoscope at admin level 1 (gadm1 identifier)
ADMIN1 Eng Name	String	Name of admin level 1
Type	Text	Event/trend/context
Subindicator	Text	List of subindicators
Indicator	Text	List of indicators
Justification	Free text	Link to the source
Source name	Free text	Name of the source
Source date	Date (DD/MM/YYYY)	Date of the source
Source link	Free text	Link to the source
Created	Timestamp	Date of entry

DATA COLLECTION

A team of ACAPS data collectors collects the data. They are trained in data collection methods, information landscape indicators methodology, inclusion criteria, and dataset structure. The information comes from various publicly available sources, including governments (official sites, embassies), media, UN agencies, news media, trade/business publications, and other organisational institutions.

ACAPS collects data daily, as the data collectors extract information from various reports. They then log the relevant information, indicating the geographical coverage and relevant population. If the source includes information relevant to multiple indicators, there are multiple entries with different indicators, and the same source is repeated. Each line in the dataset includes information exclusively relevant to one event indicator.

The collected data goes through a review process to check the completeness, validity, and reliability of the information included as follows:

Step 1: the data collectors regularly gather data to feed the information event indicators dataset.

Step 2: the reviewers check each entry that would be fed into the information landscape dataset, checking the quality of the collected information using the following criteria:

- completeness
- tidiness
- methodology consistency.