Data preparedness: connecting data, decision-making and humanitarian response

HARVARD HUMANITARIAN INITIATIVE

SIGNAL PROGRAM ON HUMAN SECURITY AND TECHNOLOGY
STANDARDS AND ETHICS SERIES 01

This paper was written by Nathaniel Raymond and Ziad Al Achkar (Harvard Humanitarian Initiative).

Graphic design by Vilmar Luiz.

Essential advice and support were provided by Martina Comes (University of Agder), Lilian Barajas, Daniel Gilman, Brendan McDonald, Kristina Mackinnon, Janet OCallaghan, Andrej Verity, Craig Williams (OCHA) and Mila Romanoff (UN Global Pulse). Casey Harrity and Josje Spierings provided input on the initial concept.

All photos provided by OCHA

CONTENTS

DATA PREPAREDNESS:
CONNECTING DATA, DECISION-MAKING AND HUMANITARIAN RESPONSE

KEY MESSAGES

- "Data preparedness" is the ability of organizations to be ready to responsibly and effectively deploy and manage data collection and analysis tools, techniques and strategies in a specific operational context before a disaster strikes.
- Data preparedness, also known as information management preparedness, is a component of broader preparedness plans. Within the humanitarian community, there are varying degrees of organizational data preparedness. The adoption of new techniques and technologies, however, requires that organizations re-think and/or develop their data/information preparedness plans to ensure they are capable of meeting today's data risks and ultimately contribute to a wider systemization of data use in the humanitarian community.
- There are five components in the data preparedness cycle:
  1. **Standard setting and risk analysis:** Standard setting involves determining what legal, ethical, regulatory and technical rules and norms govern the use of data in specific disaster scenarios. Risk analysis aims to identify the threats and liabilities that may arise in order to develop mitigation strategies.
  2. **Requirement planning and stress testing:** Requirement planning is deciding what data are needed, in what context and how they should be collected, analysed and revised, disseminated and stored. Stress testing is the process of assessing how specific disaster scenarios could affect the ability of actors to execute a data preparedness plan before an actual disaster strikes.
  3. **Coordination and consultation:** Data preparedness depends on having clearly defined and commonly agreed coordination structures specific to the use of data. Consultation is the process of sharing the data preparedness plan with key stakeholders, particularly local communities, and integrating their feedback into the plan.
  4. **Capacity-building and training:** Capacity-building is about identifying and establishing the specific skills, training, infrastructure and assets needed amongst responders and at the community level to use disaster-related data.
  5. **Evaluation and improvement:** Evaluation is a continuous process that occurs throughout the data preparedness cycle to improve individual components and the process as a whole.

WHAT IS DATA PREPAREDNESS?

Data are a central component of humanitarian response. Frequently, however, there is a disconnect between data, decision-making and response. Informed decisions need to be made in the first hours and days of an emergency, and if the elements to effectively gather, manage and analyse data are not in place before a crisis, then the evidence needed to inform response will not be available quickly enough to matter. In other words, an organization needs to be prepared to responsibly and effectively deploy and manage data collection and analysis tools, techniques, skilled staff and strategies in a specific operational context to be ready before a disaster strikes. This process is called "data preparedness". Data preparedness complements and expands on existing OCHA principles on the use of information management in disaster scenarios, such as reliability, timeliness, relevance, inclusiveness and accountability.[1]

This paper seeks to provide a blueprint for how the concept of data preparedness may be put into practice by members of the humanitarian data ecosystem.[2] This paper does not seek to replace existing Inter-Agency Standing Committee (IASC) information management practices and the Emergency Response Preparedness Framework[3], rather, to complement them by increasing awareness of one element of disaster preparedness: data preparedness.

Data preparedness is the ability of organizations to be ready to responsibly and effectively deploy data tools before a disaster strikes.

1 Tina Comes, Bartel Van De Walle "On the Nature of Information Management in Complex and Natural Disasters", *Procedia Engineering 107* (2015). Available from http://www.sciencedirect.com/science/article/pii/S1877705815010516.

2 The "humanitarian data ecosystem" comprises all humanitarian actors, their partners and affected communities acting as data producers, users and consumers (*Building data responsibility into humanitarian action*, Office for the Coordination of Humanitarian Affairs. Available from https://docs.unocha.org/sites/dms/Documents/TB18_Data%20Responsibility_Online.pdf).

3 IASC Information Management Product Catalogue https://interagencystandingcommittee.org/product-categories/information-management and Emergency Response Preparedness Framework (July 2015). Available from https://interagencystandingcommittee.org/reference-group-risk-early-warning-and-preparedness/documents/iasc-emergency-response-preparedness

Data preparedness or information management preparedness?

Within IASC organizations, the term 'information management preparedness' is more readily used than data preparedness as it was perceived that the latter placed too much emphasis on data at the expense of other elements required for situational awareness, including leadership, guidance, capacity, platforms, relationships and processes. In the IASC Emergency Response Preparedness Framework, information management is included in the minimum and advanced preparedness actions an organization should take.

For the purposes of this paper, 'data preparedness' is considered to be a subset of 'information management preparedness', recognizing that data preparedness needs to be connected to wider preparedness plans to leverage data available from development and government partners, be used in appropriate analytical models, benefit from leadership and coordination and to ensure that the outcomes of data preparedness plans are contributing to overall situational awareness.

A short history of data preparedness

Within the humanitarian community, there are varying degrees of organizational data preparedness. The adoption of new techniques and technologies, however, requires that organizations re-think and/or develop their data/information preparedness plans to ensure they are capable of meeting today's data risks and ultimately contribute to a wider systemization of data use in the humanitarian community.

Within IASC organizations, information management preparedness goes back to approximately the crisis in the Balkans (1999), where the first 'P-codes',[4] Country Operational Datasets (CODs), rapid needs assessment and analysis were done to prepare for the return of refugees from the Former Yugoslav Republic of Macedonia and Albania. An important development in the systematization of data preparedness was the IASC adoption of "Common Operational Datasets"

4 P-codes are unique geographic (geo) identification codes, represented by combinations of letters and/or numbers to identify a specific location or feature on a map or within a database (https://www.humanitarianresponse.info/en/applications/data/document/pcode-implementation). P-codes were, in a way, the pre-cursors to today's Common Operational Datasets.

Data and the World Humantiarian Summit

The Secretary-General, in his report *One Humanity, Shared Responsibility*, called for humanitarian action to be driven by shared data and analysis. This call was widely echoed at the first-ever World Humanitarian Summit, held in Istanbul in May 2016. At the Summit, Member States reaffirmed the importance of acting early to prevent potential crises from deteriorating by collecting, analysing, sharing and acting on early warning information. The Summit confirmed that it was time to shift from reactively managing crises to proactively reducing risks – a shift that must be underpinned by data and common risk analysis. Participants committed to a number of data-driven initiatives, including the establishment of the Global Risk Analysis Platform to support risk-based decision-making by synthesizing multi-hazard risk data and information; the establishment of a Humanitarian Data Centre to increase collaboration between the private sector, academia, practitioners and policymakers to improve the impact of data on humanitarian action and the UN Committee of Experts on Global Geospatial Information Management (UN-GGIM) committed to making essential baseline data available to support humanitarian preparedness, as well as operational data in the event of a response.

(CODs), in 2008, revised in 2010.[5] Since then, OCHA has assumed responsibility for identifying and making available the best datasets for each COD theme; many of which are maintained on the Humanitarian Data Exchange (HDX) and therefore available immediately. Data preparedness has been incorporated into the wider Emergency Preparedness Framework as a minimum and advanced preparedness action.[6]

However, when looking at the wider humanitarian data ecosystem, the history of data preparedness is inconsistent with organizations often developing their own ad-hoc guidelines and strategies for data collection, analysis and use in the context of ongoing disasters and delaying the deployment of skilled staff. This can lead to silos of incomplete, uncoordinated and often redundant data sets resulting from competing, impromptu data collection strategies.[7]

Why is data preparedness needed?

Humanitarians need evidence to make informed decisions about the actual needs of affected communities that will ultimately shape response. While there are many factors that drive data sharing during a response, particularly relationships with other responders, host governments and communities, individual organizations must be prepared to use data effectively and responsibly in emergencies to take optimal data-driven decisions. Data preparedness aims to mitigate negative data-related impacts by providing data collectors and users with the framework and network to be ready to work with data. For example, being data-ready can prevent or mitigate the following data-related conditions that may occur during humanitarian operations:

- **Data disparity:** humanitarian actors may have incomplete, inaccurate and/or insufficient data – whether because of a lack of a sharing relationship or because the data may not exist – to make informed decisions about the needs of affected people, which may lead to inaccurate or inequitable responses.

- **Data deluge:** the amount of data generated by responders and affected communities after a disaster may overwhelm a responders' ability to make sense of the large flows of information, negatively affecting the ability to make decisions. This often leads to uncoordinated and uncontrolled sharing without accepted protocols for verification and corroboration of data.

- **Data distortion:** improper and inaccurate analysis of data that either inflates or minimizes the severity of a disaster situation can make responses less effective and waste limited humanitarian resources.

- **Data damage:** certain uses of data, if not done in a responsible way and in compliance with data privacy and data protection laws, can cause, or be perceived to cause, harm to an organization and also to affected people and their communities. Incidents where data causes damage to affected people can break trust between partners and affected communities.

5 Common Operational Datasets are predictable, core sets of data needed to support operations and decision-making for all actors in a humanitarian response (IASC *Guidelines on Common Operational Datasets in Disaster Preparedness and Response 2010,* www.humanitarianresponse.info/en/topics/imwg/document/iasc-guidelines-common-operational-datasets-disaster-preparedness-and-response)

6 IASC, *Emergency Response Preparedness Framework* (July 2015). Available from https://interagencystandingcommittee.org/reference-group-risk-early-warning-and-preparedness/documents/iasc-emergency-response-preparedness

7 Kristin Bergtora Sandvik, Maria Gabrielsen Jumbert, John Karlsrud and Mareile Kaufmann, "Humanitarian technology: a critical research agenda," *International Review of the Red Cross* (2014), 96: 219-242. Available from http://dx.doi.org/10.1017/S1816383114000344.

Data preparedness aims to enable a better understanding of information needs, allowing more effective and responsible automated filtering, as well as better sharing protocols and processes. It seeks to support information management personnel as they manage vast and volatile amounts of data. Data preparedness also strives to ensure that the use of data for humanitarian action is consistent with the humanitarian principles.[8]

8 Raymond and Card, "Applying Humanitarian Principles to Current Uses of Information Communication Technologies: Gaps in Doctrine and Challenges to Practice", Harvard Humanitarian Initiative (2015). Available from http://hhi.harvard.edu/publications/applying-humanitarian-principles-current-uses-information-communication-technologies.

FIGURE 1:
PRINCIPLES OF HUMANITARIAN INFORMATION MANAGEMENT

Source: *Operational Guidance on Responsibilities of Sector Cluster Leads and OCHA in Information Management* (IASC, 2008)

THE DATA PREPAREDNESS CYCLE

The data preparedness cycle has five core components, each with its own subset of activities that are specific to the challenges and workflows of humanitarian data management. The five components are:

1. **Standard setting and risk analysis:** Standard setting is the process of determining what legal, ethical, regulatory and technical rules, best practices, guidelines and implicit norms may govern the collection and use of data in specific disaster scenarios. Risk analysis, begun simultaneously with standard setting, is the process of identifying what threats and liabilities may be encountered and deciding how they will be prevented and mitigated.

2. **Requirement planning and stress testing:** Requirement planning is deciding what data are needed in what context and how the data should be collected, analysed and stored. Stress testing is the process of assessing how specific disaster scenarios could affect actors' abilities to execute a data preparedness plan before an actual disaster strikes.

3. **Coordination development and consultation:** Data preparedness depends on having clearly defined and commonly agreed coordination structures specific to the use of data. Consultation is the process of sharing the data preparedness plan with key stakeholders, particularly local communities, and integrating their feedback into the plan.

4. **Capacity-building and training:** Capacity-building is about identifying and establishing the specific skills, training, infrastructure and assets needed among responders and at the community level to effectively and responsibly use disaster-related data.

5. **Evaluation and improvement:** Evaluating a data preparedness plan should occur at each stage of the cycle. Improvement structures should be put in place for capturing and incorporating lessons learnt. Evaluation and improvement are continuous processes that occur throughout the data preparedness cycle and post-disaster.

1. Standard setting and risk analysis

Why standard setting and risk analysis always come first

The data preparedness cycle must always begin with identifying, agreeing and implementing the standards that should govern the use of data as part of emergency preparedness and response. Ideally, these standards should govern operations across an organization. A risk analysis of the potential threats and liabilities of any data preparedness plan should begin in parallel to standard-setting.

These steps should precede any other action in the development of a data preparedness plan. Data preparedness planners should articulate the basic parameters and values that will govern their plan before moving forward.

Implementing data standards and conducting risk analysis is not only about preventing potential harms. It is also central to improving the quality of data-supported responses. Communicating to stakeholders which standards will apply and the potential risks that need to be managed is an essential part of data preparedness. This process helps involve local populations in the data cycle, sets expectations about what data will and will not be used and determines how actors will be held accountable for the collection and use of data. Standard-setting also is a prerequisite for any ad-hoc collaboration with new actors, such as voluntary technical organizations, that emerge during the response

Data preparedness planners should articulate the basic parameters and values that will govern their plan before a crisis starts.

What data standards should address

There are three general areas that data standards should address as part of any data preparedness plan:

- **Legal:** There are international, sectoral, commercial and national regulatory and legal standards that may apply differently depending on context, population, potential disaster and the type of data and collection platforms being used. Examples of these standards can include regulations specific

FIGURE 2:
THE INFORMATION MANAGEMENT CYCLE

to certain industries; data sharing agreements or mechanisms that activate during disasters; national regulations for specific types of data collection, as well as international and humanitarian law.

• **Ethical:** Key ethical concerns that need to be considered may include organization-specific privacy norms; what types of sensitive information about vulnerable populations and special groups like women, children, youth and ethnic minorities, will responders need and how this information will be managed taking into consideration contextual, social, cultural and other factors; who will have access to the data and how combinations of data could affect the privacy and security of particular populations.

• **Technical:** A data preparedness plan should identify what technical standards will govern the collection, analysis, storage, protection (i.e. data security) and presentation of data before an emergency occurs. Examples of technical standards can include specific formats for aggregating data, national technical frameworks for guiding mitigation and recovery work, interoperability principles and open standards and the proper use of common templates for needs assessments.

What risk analysis should address

Humanitarian actors face new risks and challenges with the rapid adoption of technologies that impact the privacy and security of affected people. Securing information is increasingly a priority for humanitarian organizations. However, encryption alone is not enough. Training in how to analyse and mitigate risk is central to data preparedness.

The risk analysis process should seek to identify the specific factors, scenarios and potential dynamics specific to each context.[9]

There are two primary categories of risk that should be analysed at each stage of the planning process and when a project is substantially changed: pre-existing risks and potential new risks. Pre-existing risks are those that exist in a specific operational environment before a plan is created. These should inform what data are collected as well as how they might or might not be applied. Potential new risks are those that may be identified specifically through the development of a data preparedness plan.

9 UN Global Pulse, "Mapping the Risk-Utility Landscape of Mobile Data for Sustainable Development & Humanitarian Action" (2015). Available from http://www.unglobalpulse.org/sites/default/files/UNGP_ProjectSeries_Mobile_Data_Privacy_2015.pdf

South Sudan – A man holds his mobile phone to the sky trying to get network access together with other internally displaced persons returning to Minkaman camp after collecting personal belongings from their former homes. The only way to travel is on barges on the River Nile. Most people cannot swim and if problems occur, there are no ways of communication since phone network coverage is limited.
Credit: OCHA/Jacob Zocherman

2. Data requirement planning and stress testing

Requirement planning is the process of determining what information from which sources is needed in a specific scenario.[10/11] Ideally, relief providers should undertake data requirement planning together to have a common baseline. This requires identifying actionable indicators[12] to develop a "task-to-tool framework".

Stress testing is the process of assessing what factors and dynamics will disrupt or prevent the execution of a plan while adhering to ethical standards and technical protocols. Stress tests challenge operational assumptions, identify weaknesses in data and communication infrastructures as well as in data collection and dissemination processes and reveal the capacity and training needs of stakeholders.

Both requirement planning and stress testing should be directly informed by the findings of standard setting and risk analysis. These processes will help determine what data is ethically and legally appropriate to collect, what risks are associated with data storage and use, and how data should be properly formatted, stored, and retained.

How to begin planning data requirements

Requirement planning starts with humanitarian actors identifying what potential disaster scenarios they might face and what are the specific data needs they will likely have in each expected situation.[13] Requirement planning will likely identify three broad categories of data relevant to a specific potential response. These categories are:

- **Baseline data**: information that provides humanitarian actors with a pre-disaster picture of the potentially affected populations, critical infrastructure, basic geography and other issues that will become crucial when disaster strikes.
- **Initial impact data:** information that will only be available after the disaster occurs, such as the severity of damage to certain structures.[14]
- **Dynamically evolving data:** information that is expected to significantly and iteratively change over time and which requires continuous data collection. This type of data is relevant in all disasters but its importance and use can vary based on the scenario.

What are the questions data requirement planning should answer?

During the data requirement planning phase, organizations must examine the concrete ways in which they will execute and manage data collection, processing, analysis, security, storage, retention, sharing and release. Key questions include:

- **Sources:** What sources will be used to collect baseline, post-event and/or dynamic data sets? Are these data sources already in place and available or will they have to be deployed? What organizations will deploy them? How is the quality of the data? Does the data need to improve? How will different types of disaster scenarios affect the type and quality of sources available? What steps should be taken to prepare for replacement or alternate sources of data if the required sources do not yet exist or are destroyed? How will new sources of data that emerge during a disaster, such as datasets produced by volunteer groups, be integrated into the plan?
- **Analysis and indicators:** Who will be responsible for conducting what types of data analysis? What standards will guide these analyses? What are the key indicators that will be extracted from data and for what decisions? What examples of past practice may be applicable? What are the competency requirements that humanitarians need to conduct the required analyses? How much time is necessary to process the data?
- **Security:** What common standards apply for data security and storage? How will these standards be enforced, updated and verified? What technical competencies and physical assets are required to securely and ethically store the data?

10 Gralla, Goentzel and Van De Walle, "Field-Based Decision Makers' Information Needs in Sudden Onset Disasters" (2013). Available from https://app.box.com/s/kneqlcpq99xlkh08w0d6

11 McCarthy, "Information Analysis: Sharing the load in the first 72 hours" (2015). Available from https://prezi.com/pwl2zhz6r9b_/information-analysis-sharing-the-load-in-the-first-72-hours/?utm_campaign=share&utm_medium=copy

12 Indicators are the actual data points that support decision-making on relief delivery: e.g. a spike in the number of refugees present in an area may support decisions about the number of temporary structures needed.

13 Gralla, Goentzel and Van De Walle, "Field-Based Decision Makers' Information Needs in Sudden Onset Disasters" (2013). Available from https://app.box.com/s/kneqlcpq99xlkh08w0d6

14 Baseline, initial damage and dynamically evolving data can also be called baseline, impact and operational data respectively.

FIGURE 3:
TASK-TO-TOOL FRAMEWORK

The scenario below shows a draft "task-to-tool" match framework focusing on post-event data needed to respond to a natural disaster. When a task-to-tool framework is developed, the data to be collected could be categorized into three broad areas: baseline data (currently defined under the Common Operational Datasets guidance), initial impact data and dynamically evolving data. Aggregate datasets, commonly used in humanitarian response, fall under the three areas and special care should be taken with these due the risk of accidentally uncovering personal or demographic identifiable information. The end goal of a task-to-tool framework is to help determine the information points, their purpose and tools to acquire data, so that responders can build evidence to make informed decisions about the actual needs of affected communities and people.

Sources: Raymond and Harrity[15] and IASC Information Management Working Group[16]

INFORMATION REQUIREMENT	PURPOSE	SAMPLE TOOLS AND TACTICS
• The number and severity of damaged structures	• Triage of most affected communities to prioritise needs assessments by ground teams	• Composite index to estimate severity ranking[17] • Analyse high-resolution satellite imagery
• Locations of critical infrastructure, such as schools and hospitals, and main roadways leading to most affected areas	• Updated, relevant maps for guiding ground teams conducting needs assessments in most affected areas	• Common Operational Datasets on Humanitarian Data Exchange • Deploy crowd mapping platforms
• Responders and capacities in-country	• Know which agencies/responders are present on the ground, and the capacities/expertise of staff to support response and coordination efforts	• Humanitarian ID[18]
• Media tracking and translation	• Understand the evolution of local conditions post-disaster and have access to local information	• Establish a reporting cycle with local Information Management Officers • Deploy Digital Humanitarian Network

15 Raymond and Harrity, "Addressing the 'doctrine gap': professionalising the use of Information Communication Technologies in humanitarian action" (2016). Available from http://odihpn.org/magazine/addressing-the-doctrine-gap-professionalising-the-use-of-information-communication-technologies-in-humanitarian-action/
16 IASC Information Management Working Group. Guidance available from https://www.humanitarianresponse.info/en/topics/imwg
17 OCHA, "Severity Estimate Ranking'. Available from https://www.humanitarianresponse.info/en/applications/tools/category/severity-estimate-ranking
18 Humanitarian ID. Available from https://humanitarian.id/

Democratic Republic of the Congo, 2012 – Data collection in the field. A World Food Programme staff member conducts a market survey in Minova.
Credit: OCHA/Philippe Kropf

- **Storage and retention:** What data will be retained by whom and for how long? What data should be destroyed? What legal and ethical standards guide retention decisions and who will make those decisions?

- **Sharing:** Does the project require data sharing? What standards apply to regulate when/how data are shared? Who can/should have access to data? How will sharing standards be agreed, communicated and enforced? Who needs to be consulted about sharing decisions?

- **Public release:** What data will be released publicly? How will these decisions be made? How will that release of data be managed and evaluated?

Stress testing a data preparedness plan

Stress testing is about checking the operational assumptions in the data preparedness plan, including identifying any infrastructure or security vulnerabilities, to ensure it can be successfully implemented. This process is sometimes referred to as "red teaming".[19] Stress testing should have two phases: (i) as part of a wider preparedness plan, ensuring that an organization can set up the structures, processes and capacities for data preparedness **before** a disaster strikes; and (ii) determining whether an organization can implement the plan's processes and standards **during** a disaster.

Stress testing should, at a minimum, answer the following key questions as they pertain to the preparedness plan:

- Can data actually be collected and processes by the capacity currently in place? Are the plan's priorities correct?

- Can data and critical indicators be corroborated? Are the quality assurance mechanisms in place sufficient?

- How secure and resilient are critical systems? Can the human resources in place manage them appropriately?

- What is the likely worst case scenario? Can the plan operate during it?

3. Coordination and consultation

Coordination and consultation are central challenges to data preparedness planning and execution. Currently, coordination around information sharing in the humanitarian sector suffers from both a "lack of mechanisms for exchanging data" as well as "a culture that resists sharing information."[20]

This problem is compounded when examining the relationship between traditional humanitarian organizations, volunteer technical organizations and local communities, where guidelines or standards for using and sharing information technology are only just emerging,[21] such as the Digital Humanitarian Network's *Guidance for Collaborating with Volunteer and Technical Communities.*[22] Without adequate policies to guide coordination and sharing,

19 Red Team Journal, "Red Teaming and Alternative Analysis" (2016). Available from http://redteamjournal.com/about/red-teaming-and-alternative-analysis/

20 UNOCHA, "Humanitarianism in the Age of Cyberwarfare" (2014). Available from https://docs.unocha.org/sites/dms/Documents/Humanitarianism%20in%20the%20Cyberwarfare%20Age%20-%20OCHA%20Policy%20Paper%2011.pdf

21 Sandvik, "The humanitarian cyberspace: shrinking space or an expanding frontier?", *Third World Quarterly* (2016), 37:1. Available from http://www.tandfonline.com/doi/abs/10.1080/01436597.2015.1043992.

22 For examples of guidelines on collaborating with online volunteer communities, see the Digital Humanitarian Network's *Guidance for Collaborating with Volunteer and Technical Communities* (2012, available from http://digitalhumanitarians.com/content/guidance-collaborating-volunteer-technical-communities) and *Guidance for Collaborating with Formal Humanitarian Organizations* (2013, available from http://digitalhumanitarians.com/content/guidance-collaborating-formal-humanitarian-organizations)..

Nepal, 2015 - In the first few weeks after the earthquake, hundreds of affected people charged their phones on makeshift phone charging banks. Phones are used for more than calls in Nepal, with people using them to also listen to radio. Credit: OCHA/Stewart Davies

humanitarians risk "turning … into threat actors in cyberspace."[23] To prevent becoming threats, humanitarians involved in data preparedness must prioritize developing inclusive coordination structures that are built on consultation with key stakeholders, in particular, local communities.

Building effective data preparedness coordination and consultation structures

Factors that will affect the degree of coordination and consultation that is possible include the type of disaster, the lead responder, e.g. national governments or an INGO, as well as the permissibility of the environment for humanitarian actors. Regardless, the following five principles usually apply in all circumstances:

- **Communicating the purpose and benefit:** as much as the context permits, coordination structures should serve to receive feedback from affected populations about the purposes for which it is appropriate to use data about them before it is collected and the expected benefit to be gained from using such data.

- **Responsibly managing critical incidents:** when critical incidents involving data occur, such as a data breach, it is critical to have mitigation mechanisms to address such incidents in a timely manner. Coordination and consultation structures can bring together the necessary stakeholders and technical experts to respond quickly and appropriately to critical incidents, integrating lessons learned into the data preparedness plan.

- **Roles, rules and responsibilities:** data preparedness depends on each participant in a plan being clear about individual roles, rules and responsibilities, as well as those of the other implementing groups.

- **Common inventory and common formats:** coordination structures should be the repository for common inventories of what data are available before and after disaster strikes, as well as deciding at what level that data repository will be established and managed. Ideally, these should include and be based on current Common Operational Datasets (CODs).[24]

- **Combining contextual knowledge with technical expertise:** coordination of data preparedness plans is challenging because it often involves integrating diverse groups of technical experts with humanitarian actors rooted in specific cultural and operational contexts. Successful data preparedness coordination effectively integrates technical and humanitarian actors.

4. Capacity-building and training

Several types of general and specialized capacities need to be in place to develop and execute a data preparedness plan. Relatedly, training regimes for executing data preparedness operations are a mix of general disaster preparedness exercises with data-specific elements.

23 Sandvik, "The humanitarian cyberspace: shrinking space or an expanding frontier?", *Third World Quarterly* (2016), 37:1. Available from http://www.tandfonline.com/doi/abs/10.1080/01436597.2015.1043992.

24 CODs and Fundamental Operational Datasets (FODs) are datasets used in humanitarian emergencies, which OCHA identifies, publishes and maintains (https://sites.google.com/site/ochaimwiki/cod-fod-guidance). CODs/FODs undergo regular reviews and once local Information Management Working Groups agree on them, they are uploaded to the Humanitarian Data Exchange (https://data.humdata.org/).

FIGURE 4:
TYPES OF DATA PREPAREDNESS TRAINING

TRAINING METHOD	DESCRIPTION
Simulations	Simulations assess the ability of all stakeholders to execute the plan and help identify gaps in capacity.
Forecasting and developing analytical models	Simulations with existing or new analytical models that incorporate a number of datasets to produce information on humanitarian needs in a particular context.
Spot drills	Spot drills test one specific technical or operational component of the plan, such as a mapping or survey team.
Data and asset inventories	What data collection and analysis assets are both in place and needed.
Security audits	Unannounced tests to ensure that physical infrastructure, such as servers and networks, are secure and well maintained.
Technical trainings	Trainings focused on specific technical competencies that responders need to have to execute the data preparedness plan.
Outside reviews	Independent experts, usually within one specific technical area, examine the plan and provide critical feedback.

Types of capacities required for data preparedness
Notwithstanding context-specific capacities, below follow examples of the six types of common capacities that data preparedness planners and community-level partners need to identify, develop and maintain:

- **Data collection assets:** the physical tools and platforms with which data will be collected. Building the capacity of responders specific to data collection assets can range from the actual acquisition of assets and ensuring access to their products (e.g. unmanned aerial vehicles and location-specific satellite imagery) to pre-positioning of tools (e.g. smartphones for use by survey teams).

- **Human resources:** the use of data collection assets will only be as successful as the development of the human resources capacity to responsibly and effectively use them. This includes training staff to use analytical models to translate data into humanitarian needs and operational plans.

- **Infrastructure:** includes telecommunications networks, servers and hard drives, software(s), facilities and transportation resources that will be required to execute the plan. A core part of building infrastructure capacity includes "worst-case scenario" planning to ensure that data preparedness plans operate in different disruption contexts in which part or all of the necessary capacity is wiped out. Continuity of operations and system security depends, in large part, on appropriate infrastructure planning.

- **Quality assurance:** quality assurance (QA) capacity can often be one of the most critical, politically sensitive and time-consuming capacity to have in place, yet it is often one of the least developed. QA capacity requires designated human resources and clearly defined proce-

dures to be developed, tested and trained before disaster strikes. QA can ensure that the ways in which data are collected, analysed and utilized adhere to technical, ethical, and legal standards.

- **Technical competency:** technical competency is a basic part of human resources capacity-building but extends beyond knowing how to work with software, for instance, to relationship-building and communication, among others. Technical competency often requires bringing in technical experts to train key staff about how to use certain data-related tools and techniques, for example, how to conduct surveys, make maps, analyse datasets, use imagery from satellites and store data appropriately.

- **Monitoring and evaluation:** organizations should ensure that monitoring and evaluation occurs at each step in the data preparedness cycle to improve individual steps and the plan as a whole. Monitoring and evaluation will help identify, for example, if the standards setting process is initially successful, but there is a lack of capacity to implement the standards.

5. Evaluate and improve

Data preparedness, as with any other area of humanitarian action, requires evaluation to be incorporated into each stage of the planning cycle as a constant and consistent feedback loop. Two of the most important moments for improving data preparedness are the outcomes of any training exercise and any time the plan is executed during an actual disaster. Particularly for the latter, there should be agreed procedures for immediately capturing and responding in real-time to any critical incident that may occur as part of the execution of a plan.

Questions when evaluating data preparedness planning

- **Standards:** Did the organization identify the correct set of standards applicable to its proposed use of data? Did all stakeholders have the training and capacity to uphold the standards? Were new standards identified or created during the data preparedness cycle? What additional resources are required to improve standard identification, adoption and accountability? Did new, unforeseen risks emerge that need to be integrated into the plan's risk analysis?

- **Data requirements planning:** Were the plans appropriate to the disaster scenario? Did reflect actual needs of all stakeholders during the response? What evidence is there that the plan did or did not help improve the response? Were the proper collection tools, analytic techniques and data indicators used?

- **Coordination:** Did all actors understand and execute their specific roles within the plan? Were the roles assigned to various actors appropriate? How can decision-making about the collection, analysis, storage and release of data be improved?

- **Capacity:** Did actors have the resources necessary in terms of assets, staff and technical competency? What areas require further investment and commitment to improve?

- **Training:** How did the training influence the actors' response and planning? Were the trainings beneficial and representative of the expected needs?

CONCLUSION AND RECOMMENDATIONS

As the humanitarian community works to address complex challenges it faces specifically related to data, data preparedness becomes an essential framework for this discussion. The adaptation of current coordination structures should be directly informed by the issues raised by data preparedness.

To professionalize the use of data in humanitarian action, there are four priorities for humanitarians:

- **Agree on baseline data and a model/shared analysis for translating data into needs:** the development of generally accepted, evidence-based criteria for what types of baseline data are needed when and where, ideally based on current CODs, will significantly advance international, national and local level data preparedness.

- **Strengthen relationships between data producers and humanitarian actors to improve data collection:** often, development partners and host governments already produce the baseline data that humanitarians require. With strengthened relationships and a framework for sharing data responsibility – together with a commitment from governments to make essential baseline data available to support humanitarian preparedness – data collection can be improved.

- **Adopt minimum standards for data preparedness planning:** data preparedness planning should be a core competency of humanitarians. Responders should receive training so they know, in advance, where/how to request data or analysis, for what purpose and to meet what outcome. The ultimate aim of minimum standards is to ensure that all actors achieve a basic standard of competency for integrating data into response plans before disaster occurs.

- **Create a common data standards and risks toolkit:** Humanitarian actors lack common resources for addressing the complex and situationally specific ethical, legal and regulatory issues they face across contexts and scenarios. A common toolkit of resources and a basic checklist of issues can help guide practitioners and voluntary technical organizations when navigating these challenges to mitigate risks and set standards for employing a data-driven response.

For data and shared analysis to become the bedrock of humanitarian action, as envisioned by the Secretary-General in his report *One Humanity, Shared Responsibility*, the humanitarian and development communities will need to rally together to build preparedness plans to better connect data and decision-making.