# Data Management in Emergency Response: Observations from the Field During COVID-19 and Storm Ana

Kenny Meesters
Tilburg University
k.j.m.g.meesters@tilburguniversity.edu

Olaf Steenbergen
International Federation of Red Cross and Red Crescent Societies
olaf.steenbergen@ifrc.org

Yan Wang
Delft University of Technology
y.wang-16@tudelft.nl

## Abstract

*During disruptive events, the exchange of information is a key factor in successfully managing the adverse effects. Today, there is a plethora of data and related data-technologies available for emergency response organizations, which can help address the information needs. Data has a great potential to support responders in their operations, especially in complex emergencies with longer lasting and more widespread effects. However, the increasing availability and use of data in emergency response also presents new challenges. The emergence of data in the field of crisis response is not only technical in nature, but also has impacts on the organizational aspects. Drawing on existing literature and best practices in data management and governance activities, we explore this topic in two cases centered around large-scale emergency responses. Data-management challenges faced by responders are observed first-hand and implications are identified for successfully leveraging the potential of data in the immediate responses to large-scale emergencies.*

**Keywords:** Data management, Crisis Response, Information Management, Coordination, Governance.

## 1. Introduction

In times of crisis decision makers are faced with a high degree of uncertainty. In these situations, having timely, relevant, and accurate information is crucial to effectively manage these situations (de Goyet, 2008), such as for the identification of needs or the allocation of the appropriate resources. However, this critical information can be hard to come by, especially in complex, dynamic disaster contexts.

At the same time general and in particular technological advancements over the past decades have led to the emergence of a 'Data-Society' (Kitchin & society, 2014). Increasingly data is being generated, stored, and shared in all facets of our society, no longer being a niche for software engineers, data scientists, or experts. In fact, data has become a commodity for organizations, governments, and society at large. Even when data is not available, an increasing number of tools, resources, and possibilities allow us to gather new data or collate data from an increasing number of sources. Moreover, the advancements in information and communication technologies are further accelerating these developments and increasing the role of data in our society (Lissenden, Maley, & Mehta, 2015).

These technical developments and the importance of data has been recognized by various crisis response and humanitarian agencies, exemplified by the development of various initiatives to support organizations in gathering, using, and disseminating data over the past years (Ashish et al., 2008; Coyle & Meier, 2009). In addition to general (commercial) solutions, bespoke systems and approaches have also been introduced into the crisis management domain. New technologies (e.g., crowd-sourcing techniques, social-media analysis, and mapping) support the generation and collection of data in crisis situations (P. Meier, 2011). Developments such as the Humanitarian Exchange Language (HXL), the International Aid Transparency Initiative (IATI) provide data standards to increase the interoperability of data. While platforms such as the Humanitarian Data Exchange (HDX) and the GO-platform of the IFRC facilitate the dissemination and exchange of data.

### 1.1. Problem Statement

Despite these advancements, the increased possibilities of data to support the informed decision-making process, challenges remain to effectively leverage this potential (Clarke, 2016; Woods, 2002). While the potential of data management in emergency response is often recognized, it is still considered a niche. Often, data management activities are ad-hoc organized, in part because the lack of an existing, well-defined infrastructure due to volatile and dynamic operational circumstances (P. Meier, 2015; Sharma, Joshi, & Management, 2019). Existing structures and frameworks only provide support to a limited degree as they need to adapt to local circumstances, which also impacts the nature of the data managed. Furthermore, data management activities are often separated in dedicated sub-teams. This complicates data management, especially during the immediate and initial response, generally characterized by a data-gap and

URI: https://hdl.handle.net/10125/102858
978-0-9981331-6-4

a fluid 'data-landscape' (Bharosa, Janssen, Tan, & Work, 2011; Van De Ven, van Rijk, Essens, & Frinking, 2008).

In these early stages of an emergency, implementing procedures, work-agreements and structures are vital to establish effective emergency response and coordination operations. This is also the case for the collection, use and sharing of data. Thus, laying the infrastructure (i.e., the modality to collect, use, and share data) in these early stages, without specifying the exact data to be managed yet, is considered an important step in crisis management to facilitate the exchange of data between stakeholders. Although guidelines and best practices for data-management have been established and even researched, crisis management adds a layer of complexity to data management, and vice versa managing data adds complexity to the crisis response. While acknowledging the role of the type, quantity, volume, sensitivity, and other characters of data in this bi-directional relationship, the facilitation of data exchanges from a more operational and thematic perspective needs further exploration. This can be considered as one of the prerequisites for data and information management during crisis response, which requires a better understanding of the key components in the organization of crisis response and coordination that allow us to effectively leverage the potential of data.

### 1.2. Research objective & approach

The work presented in the rest of the paper aims to identify the complexities and challenges those stakeholders encounter in data management with respect to the net-centric environment and explores the influential factors to the management and exchange of data in the given context. We explore this subject through two theoretical lenses: the internal organization during crisis response, and the overall approach to data management, including governance categories. We bring the combined view into the cases of COVID-19 and Storm Ana and discuss findings with respects to data management practices and challenges (fig 1). Each case brings a unique perspective on the approach to data management, one from a more slow-onset crisis and the one from a sudden-onset crisis. This reflects the author's recognition of the importance of the context on the effectiveness of data management practices.

## 2. Theoretical background

### 2.1 Crisis management

Most often, crises are the result of a disaster event, which is (1) sudden, (2) seriously disrupts routines of systems, (3) requires new courses of action to cope with the disruption, and (4) poses a danger to values and social goals (Coombs, 2021; Quarantelli, 2005). As an agent of disturbance, a disaster often triggers an escalatory process that undermines a social system's capacity to cope with its consequences (Buchanan-Smith & Maxwell, 1994). For this reason, crisis management requires taking decisions that should have the effect of restoring this social order, as well as of minimizing the loss of life and damage (McConnell & Society, 2011). This, however, is extremely complex, especially as the exact triggers and underlying causes of the subsequent crisis are not always easily identifiable (Buchanan-Smith & Maxwell, 1994). In addition, the decision-making capacity of crisis managers is limited due to time pressure, scarce resources and capacities, and a lack of knowledge about the situation at hand (Meesters, 2021). The combination of being under time pressure to act with a high level of uncertainty and the ambiguity of actions forms the central challenge to crisis management (van den Homberg, Meesters, & Van de Walle, 2014).

Situational awareness is crucial for crisis managers to make decisions. This concept encompasses not only a degree of awareness regarding the presence of relevant elements in the environment and a comprehension of the crisis situation, but also a projection of its future status (Endsley, 2001). Information plays a crucial role in facilitating this awareness through lowering the uncertainty and ambiguity for a crisis manager. The higher the situational awareness, the better crisis managers are able to allocate resources and coordinate actions, which are the two central objectives of crisis management decision-making (Luokkala & Virrantaus, 2014). Establishing situational awareness requires high quality information

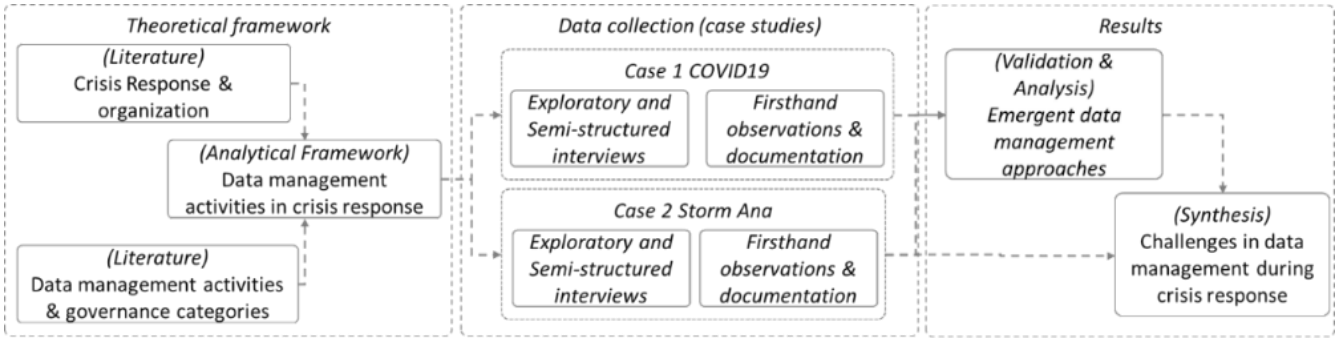


**Figure 1. Research approach**

which in turn requires obtaining relevant, accurate, and timely data, either through the primary collection or from other organizations (Gralla, Goentzel, & Van de Walle, 2015). One of the primary challenges alongside ineffective communication and issues regarding resource allocation, according to Reddy et al. (2009) is the management of information, which has the potential to cause coordination breakdowns between teams. This is exacerbated by the fact that the relevance of data rapidly diminishes during crises, especially in its acute phase (Baharmand, Boersma, Meesters, Mulder, & Wolbers, 2016; Y. Wang & Meesters, 2020). The combination of these two challenges influences the decision-making capacity of crisis managers across teams involved, being dependent on a high-quality, structured flow of information. This, in turn, spurs the need for a consistent, structured approach to data management, a need that is constant throughout all phases of a crisis. However, data Management becomes extremely challenging due to the increased time pressure, scarce resources and capacities, and high ambiguity in the acute phase of a crisis. Although information requirements at this stage may be clear, there are often gaps in the information flow between crisis response organizations, for instance regarding the availability of data (i.e., what organizations are in possession of, or require, data), the standard data structures to use across teams, or the presence of data governance mechanisms (Rodríguez et al., 2007). These gaps, in turn, do not only obstruct the effective sharing of information but also create challenges with regard to determining legal requirements, privacy issues, and other organizational considerations. In the acute stage of a crisis, these data management are key prerequisites to establish effective, reliable, and sustainable data flows to support the decision-making process.

## 2.2 Data management practices

Data management is the operational practice of properly handling data in a responsible way. It helps to organize data with respect to all relevant concerns and ensures the sustainability of data during and its life cycle (Yoon, Aiken, & Guimaraes, 2000). Data management tasks are closely related to the activities where stakeholders are involved and interact regarding the processing and exchange of data. Despite the variety of the lifecycle models due to institutional specifics (Ball, 2012), common phases are identified around the activities of collecting, processing, analyzing, storing, disseminating, and archiving data. It is also a continuous and integrated process that systematically addresses considerations from multiple aspects and ensures the stakeholders involved can handle the data accordingly.

Adopting appropriate data management practices surpasses the operational nature centered around the management of datasets. The importance of various aspects in relation to data management has been well recognized by studies on data governance (Cheong & Chang, 2007). The data governance principles contribute to identify several crucial considerations for responsible data management (Brous, Janssen, & Vilminko-Heikkinen, 2016). It requires good **technical** care of data (i.e., proper organization, reliable storage, version control, encryption). It also asks for an **organizational** arrangement to establish accompanying processes and protocols. Licensing and ownership of data has also received increasing attention and its **legal** impact needs consideration in data management as well. Furthermore, the extensive implementation of Internet of Things (IoT), Artificial Intelligence (AI) and citizen science in daily life has been exploiting a wider range of resources for data collection, some of which may intrude on the **privacy** of individuals and cause ethical issues (Stahl, Wright, & Privacy, 2018). Checking whether data exchange activities are compliant with relevant regulations is also part of the data management responsibilities. A data management concept note (Wang et al., 2020) was created to incorporate the abovementioned issues within a multi-stakeholder environment that identifies four core phases of data exchange activities across organizations (acquisition, collection, sharing) and within individual organizations (storing / backup). The note also covers related issues in data management from different aspects. Table 1 presents a mapping between the data management phases, the activities performed in each phase and the governance categories of issues each activity addresses.

**Table 1. Data Management activities & classifications**

| Phase | Data management activity | Category |
|---|---|---|
| **Data acquisition** (Al-Khouri & Technology, 2012; Wiles et al., 2008) | Check data ownership<br>*Clarify ownership, attribution and use conditions of data* | Legal<br>Organizational |
| | Check data confidentiality<br>*Regulatory compliance for processing sensitive data* | Privacy<br>Legal |
| | Check data type, format, size<br>*Determine tools and infrastructure for data processing* | Technical |
| **Data collection** (Meesters et al., n/a) | Est. data collection workflow<br>*Allocate resource for data collection* | Technical<br>Organizational |
| | Arrange storage<br>*Ensure the availability and security of storage facility* | Technical |
| **Data storage / backup** (Bell, et al., 2017) | Create folder structure and file naming convention<br>*Standardize data organization* | Technical |
| | Control access to data<br>*Implement access protocol and protection to confidential data* | Technical<br>Organizational |
| | Version control of data files<br>*Create transparent data file history* | Technical |
| | Determine min. data documentation<br>*Explain how the data can be traced, understood, and used* | Technical |

| | | |
|---|---|---|
| **Data sharing** (Fitzgerald, **2009)** | Create data sharing procedure<br>*Assess data sharing with other parties in compliance with all relevant regulations* | Organizational<br>Privacy |
| | Data copyright & licensing<br>*Determine and ensure attribution during data sharing* | Legal |

## 2.3 Conceptual model

Notwithstanding preparatory activities such as training, the development of emergency plans, or adapting new opportunities, crisis management is characterized by dealing with unknown situations, complex actor-landscapes, and volatile operational circumstances, requiring a certain adaptability and flexibility. On the other hand, data management activities and related governance aspects are often more diligently designed and well-considered in the implementation. In short, on the one hand data-management calls for a structured, considered, continuous approach, while crisis management faces a volatile environment, time and resource constraints and a high cognitive load.

Nevertheless, the same data management activities - and related challenges- occur from the acquisition and safe keeping of data to the ethical and legal considerations. These challenges are closely related to the setup, policies, and management of the crisis response (i.e., team). For example, the legal framework of the response also informs the judicial basis for data management. Similarly, the choice to deploy or use certain technologies is not only driven by the requirements for data management but heavily influenced by the team composition and the capabilities & capacities. We therefore aim to explore these challenges through these *cross-cutting governance aspects,* as outlined in Table 1 and visualized in Fig 2.

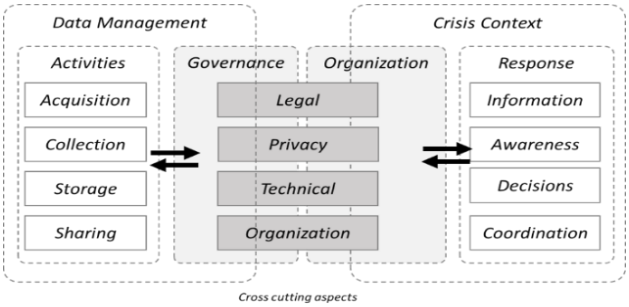


**Figure 2. Conceptual model**

# 3. Research method

A case-study approach was followed to capture different actors developing and implementing their data management activities (Yin, 2012). The cases used include large-scale emergency responses involving a large number of actors. These actors each have their own information needs, as well as data to share. The first case is the 2022 Storm Ana and the international response that followed involving many different organizations, including international agencies, rescue teams, national capacities, and community efforts. The second case is the response to COVID-19 in the Netherlands. The pandemic and its widespread impacts on social, economic, governance, and safety aspects of society forced a reconfiguration of crisis management structures and resulted in an unprecedented complex environment.

## 3.1 Data collection & Analysis

In both cases, research was conducted through semi-structured interviews and conversations with a variety of actors (Chan & Comes, 2014). We have employed an interview protocol to allow participants to describe their data management approach from a practical and anecdotal narrative, and ensure answers grounded in the (case) reality. Both cases focus on a similar set of information management aspects, this does allow for a qualitative comparison and a shared interview protocol, shown in Table 2. The interviews were further supported by direct observations and firsthand experiences from the researchers using a participatory research approach. This included attending and participating in various activities such as meetings, assessments, and discussions with different actors.

**Table 2. Data collection & analysis protocol**

| Topic | Description |
|---|---|
| Introduction | Biographical information of the interviewee, the mandate, objective of the organization or team, and the specific role in the crisis response. |
| Data needs & offers | Organizational data needs and supply related to the information needs and required decision-making. |
| Data activities | Specific activities undertaken to obtain, collect, store, and share data, incl. motivations behind. |
| Data challenges & development | Problems encountered in executing the data management activities and actions/interventions undertaken. |
| Reflection & closing | Other relevant contributing factors and lessons learned. |

The interviews have been transcribed and analyzed to identify key data management activities that took place during the crisis response in accordance with the model presented in Table 1. For each case study and activity, we also identified the information that actors sought after as well as information that they had available. To validate the classification applied to the interview-data, we conducted secondary data analysis using internal notes and public

reports for each of the cases. Next, we classified the activities according to the model introduced and expanded the analysis with additional information obtained from the interviews according to the analysis grid from Table 1 and Fig 2.

### 3.2 Research data collected

Research data for both cases was collected over a two to three-month period as part of either an ongoing research project regarding the role of information in regional and national crisis responses (case 1) or as a stand-alone exercise (case 2), both as action research (Avison, 1999) alongside active response operations. The authors were called on short-term missions as information manager (IMO) and information management coordinator (IMC). This enabled both researchers to observe the establishment and evolution of data and information management processes and tools. In addition, fellow crisis responders were interviewed, and related policy documents and guidelines were studied. The above-mentioned framework (Fig 2) was used to catalogue the data from these interviews and document analysis, while the resulting analysis was reflected upon from personal experience, observations, and conversations.

**Table 3. Summarized interview/research protocol**

| Research Data Collection | | |
|---|---|---|
| | **Case 1: COV19** | **Case 2: Storm Ana** |
| Time-period | 3 months: Mar-Jun 2020 | 2 months: Feb-Apr 2021 |
| Interviews | 4× Information managers<br>3× Team/Org. leaders<br>2× Technical support<br>5× Team-members/experts | 2× Response coordinators<br>3× Team members |
| Meetings (participant) | 10× Team meetings<br>5× Interagency meetings<br>5× Bilateral meetings | 15× Team meetings<br>10× Interagency meetings |
| Activities (observer) | 4× Interagency meetings | 5× Interagency meetings<br>3× Needs assessments |
| Document review (examples) | Technical policies and docs; daily briefings/updates; weekly management reports | Technical policies and docs; daily briefings; sporadic reports |

## 4. Case 1: COVID-19 in The Netherlands

In early 2020, the first COVID-19 cases emerged in the Netherlands during the time in which most of the countries were enjoying the holidays. Traditionally in this holiday period, Dutch people go on ski holidays or celebrate "Carnival" a pre-Lenten celebration in the southern part of the country. These movements led to a major surge in COVID-19 cases, rising from the first case on February 27, 2020, to 14,000 cases one month later. On March 16, the prime minister issued the order for an "intelligent lockdown." At the same time, the emergency services enacted their second highest response level (Kuiper et al., 2020).

Since the spread of the virus grew exponentially, the national government decided that measures would require coordination on a national level and established a new coordination structure. This organization was established to form a bridge between the operational and policy aspects of the response and positioned at the nexus of operational agencies, the national government, and regional safety boards. A key aspect was to facilitate the exchange of information among the different partners. In this role, it evolved into a key coordinating body in the Netherlands. As the pandemic and its effects continued to spread across the country, the number of involved organizations in the response also increased. At the same time, the organization also started to develop more intense collaborations with key partners, among others to exchange data regarding the COVID-19 response, such as regarding public health facilities, the number of daily infections, and the movement of people during periods of lockdown.

### 4.1 Results

**Data acquisition:** Initially, data was mainly obtained through pre-existing personal and professional relationships and on an ad-hoc basis. Main agreements for the transfer and ownership of data were based on trust as agreements on data ownership were absent. causing most information in the early stages to be acquired without clear confidentially classifications. The data formats of the data covered a wide range of formats, ranging from structured, machine-readable formats to text documents, presentations, and PDFs. This depended on the contents and source, such as if it had already been processed and shared as reports or maps.

**Data collection:** In the early stages, people within the organization used their own systems to store the data, including personal accounts on commercial data storage platforms, enabling team members to quickly get started. While other solutions were available, these would prove more cumbersome to use as it required reconfiguration of systems, or people were unfamiliar with the tools. Later, a centralized system (MS Teams) was introduced along with support to users. A key aspect in the structured collection and storage of the data were clear procedures and tools to be used. Especially during crisis situations, the capacity of installing, familiarizing and effectively using new tools is limited. Support, training, and guidance is key to adoption.

**Data storage:** A challenge for the data storage and backup was the use of personal devices. This 'bring-your-own-device' also meant that people used different software. While this proved beneficial for productivity in the early stages, it made the coordination and alignment of the procedures, settings increasingly challenging as both the organization and amount of data grew. Furthermore,

each sub-team within the organization had its own shared standard for organizing data or files. File naming was used as a basic form of version control, and backups were not explicitly considered. Finally, a common frame of reference for cataloging materials beyond folder-structures and filenames was not available. This limited the use of metadata and cataloging options to store and index data.

**Data sharing:** The processed data was published at irregular intervals, for example to the national crisis management information system whenever updates became available. Later more specific information products were defined that would be produced at regular intervals for specific audiences. These included situational updates, status monitors, and dashboards. Additionally, data was also shared based on request from external stakeholders. These would be one-time requests serving a specific or temporary information need. In the early stages, data was mainly provided (and acquired) based on specific requests. Over time, recurring request were bundled in for example weekly updates. Eventually the organization also began pro-actively determining and anticipating the data needs and subsequently developing related data outputs. Furthermore, new services were emerging to accommodate a wider range of data needs and related activities, including trend analysis and geographical breakdowns.

## 5. Case 2: Tropical Storm Ana

On the 24th of January 2022, Tropical Storm Ana made landfall in the southern and central districts of Malawi, causing heavy rains and strong winds that would put over 990,000 people in Malawi in urgent need of humanitarian assistance. Soon after, the Government of Malawi activated a 'cluster approach' used in previous disasters, leveraging on existing institutional arrangements to coordinate the response. Each cluster would consist of different agencies, including the UN, government agencies, and NGOs with expertise and experience in specific sectors. As one of the primary mechanisms of the cluster approach, an Inter-Cluster Coordination Group (ICCG) was instituted as the governing body responsible for providing technical guidance and coordination for operational aspects. This group consisted of delegates from each cluster with the key coordination priorities to provide information management, communication, and reporting. In particular, the ICCG instigated a separate Information Management (IM) Working Group. One of the authors has been active in this group as the IM Coordinator.

### 5.1 Results

**Data acquisition:** As many institutional arrangements were already in place for the ICCG, the group was quick to mobilize. At this point in time, however, there was still a high degree of ambiguity regarding data availability. Early decisions were made based on a combination of the scarce data collected by districts and organizations, as well as publicly available data. Members of the ICCG would often reach out separately to districts and organizations to acquire data, a process that lacked coordination. Although there was a general understanding that most data were confidential, no agreements were made on the ownership of data. The districts acquired data in a structured manner by using government standards, while other data would often be unstructured and of various formats.

**Data collection:** Initially, the ICCG and IMWG would request agencies to collect primary data, mainly needs and damage assessments. This would rely on the deployment of inter-organizational teams that would visit households in affected areas, while there were also substantial organization-specific efforts to collect data on more specific indicators, such as health (e.g., the quality of hygiene facilities in camps) or shelter (e.g., the number of houses made inhabitable). In the latter case, data collected would often only be shared during meetings and, as communication with districts and organizations was not tracked or monitored, different members of the ICCG would regularly request data. Conversely, data collected by inter-organizational teams was compiled by the Government of Malawi and distributed to organizations. The main issues here was the lack of metadata, common data definitions, as well as other data standards.

**Data storage:** Although the need for a central data repository was apparent, data was being stored on separate storage solutions as members used their organization-specific software and devices. In addition, common file naming conventions were not used, and the use of back-ups and version-control would depend on the (commercial) supplier of the storage solution. The lack of naming conventions created ambiguity across the ICCG regarding the documents and versions in use, which became apparent in later phases in discussions regarding the accuracy of figures within the ICCG. A centralized data storage solution was introduced in reaction, but generally used only by a selected number of members. Central guidance regarding data storage would not be established throughout the crisis as members preferred other means for storage.

**Data sharing:** Data would be published in reports (e.g., situational updates) at regular intervals to support the decisions of the ICCG and of all other agencies involved in the response. The majority of the IMWG's outputs, however, would be ad-hoc, especially in the earlier stages of the crisis. Although these requests would present in every phase, the proportion of ad-hoc requests compared to recurring outputs would decrease over time as most information needs would be established. As a coordinating body providing oversight, the ICCG would become the central place for districts and organizations involved to acquire information regarding the crisis.

# 6. Findings

While the two cases took place in different contexts, there are similarities regarding data management challenges. In both, data played a crucial role in establishing situational awareness and supporting decision-making. Nevertheless, a key distinction between the two cases that has become apparent is the use of pre-existing structures in the case of Tropical Storm Ana, designed and based on previous, similar emergencies, especially regarding the rapid formation of the coordination body. Standard procedures and systems provided a common ground to start from but proved rigid at time. The establishing and structuring the coordination mechanism in the COVID-19 case presented challenges but allowed more flexibility to adapt to the unique needs of the crisis.

## 6.1 Data Acquisition

During crises, time pressure, limited resources, and ambiguity cause the data acquisition phase to be ad-hoc and reliant on personal connections of members of the organization. While this does allow for a level of flexibility, it causes a general lack of agreements regarding the ownership of data and standards. Pre-existing structures in the second case study, however, allowed for the use of standardized indicators, something not yet available in the early stages of the COVID-19 case study. At the same time, there would be less ambiguity regarding available data.

**Table 4. Key data acquisition issues from the cases**

| Data Acquisition Issues | |
|---|---|
| **Case1: COVID-19** | **Case 2: Storm Ana** |
| • Ad-hoc and rely on personal connections (*organizational)*<br>• Ownership not established and lack of agreements (*legal, organizational)*<br>• Wide range of formats and key indicators were in use (*technical)* | • Ad-hoc *(organizational)*<br>• Ambiguity regarding data availability *(technical, organizational)*<br>• Lack of agreements (*privacy, legal, organizational)*<br>• Data formats and definitions (*technical)* |

## 6.2 Data Collection

Similar to the data acquisition, the data collection phase is characterized by an ad-hoc nature as central solutions to data storage and data workflows would yet to be implemented in the early stages. One of the major reasons was the use of different solutions and private accounts, which also resulted in a general lack of metadata. In the later phases of the COVID-19 case study, a workflow would be established allowing better coordination, while this would not be established in the other case study.

**Table 5. Key data collection issues from the cases**

| Data Collection Issues | |
|---|---|
| **Case1: COVID-19** | **Case 2: Storm Ana** |
| • No data classification (meta-data) or index (*organizational)*<br>• No centralized storage solution and workflow (*technical, organizational)*<br>• Private accounts / public services used for storage (*privacy, legal)* | • Decentralized, no central workflow *(technical, organizational)*<br>• Lack of metadata (*organizational)* |

## 6.3 Data Storage

Different storage solutions were used, often a combination of local and (commercial) cloud-based solutions. This made it difficult to make agreements on access and version control, naming conventions, and file structures. A centralized storage solution would only be introduced in a later phase of the crisis, although the acceptance of this solution was low in one of the cases.

**Table 6. Key data storage issues from the cases**

| Data Storage Issues | |
|---|---|
| **Case1: COVID-19** | **Case 2: Storm Ana** |
| • Version control not used (organizational, technical)<br>• No centralized access control or audit (*legal, organizational)*<br>• Lack of agreed standard for file structures and indexes (organizational) | • Decentralized, no central repository (technical, organizational)<br>• Lack of guidelines for naming conventions and guidance regarding the use of storage solutions (organizational) |

## 6.4 Data Sharing

In the early stages, dissemination flows for the sharing of data were not established in both cases as data would most often be shared on an ad-hoc basis. Later, as information requirements became apparent, information and data would be shared in regular intervals through the use of information products, such as dashboards.

**Table 7. Key data sharing issues from the cases**

| Data Sharing Issues | |
|---|---|
| **Case1: COVID-19** | **Case 2: Storm Ana** |
| • Strong need for profiling and no established dissemination flow/pattern *(organizational)*<br>• Sharing products instead of source data (*technical, organizational)* | • Ad-hoc sharing of data – upon request, or opportunity-driven *(organizational)* |

# 7. Discussion

Across the two cases, there is large overlap in the (types of) data management issues encountered by the organizations. Most notably, the majority of issues that would hinder an effective management of data are organizational by nature rather than legal, privacy, or

technical challenges. In both cases, data management practices evolved from an ad-hoc formed, decentralized, and pragmatic approach towards data management to a mature organization employing various techniques, tools, procedures, and policies for the management of data. A variety of reasons explain to which extent data management would be able to shift towards this higher level of maturity. Here, challenges were primarily outside of the legal, privacy, and technical realms, which is why these aspects will not be elaborated upon in full. Rather, we focus on the aspects that impact the ability to mature: the organizational aspects.

Over time, a continuous, growing need for data spurred the development of more structured approaches within the organization depending on the frequency and granularity of the required data. As did the technical possibilities, often dependent on the available data sources. The above-mentioned results imply various design considerations, implementation concerns, and management challenges related to data management practices. Specifically, we can discern the follow common main causes for the challenges listed in the previous section:

- **The emergence of temporary organizations and coordination structures *(organizational)*:** required to continuously adapt to the evolving crisis situation complicates coordinating data exchange activities in terms of managing relationships among the involved parties to ensure data availability.
- **Diverse, and multi-disciplinary team compositions *(organizational)*:** members with diverse backgrounds and expertise had different perspectives and best practices on data management, complicating the implementation of centralized solutions.
- **Technical possibilities *(technical)*:** although technical options regarding data management are numerous, successful use in crises require careful implementation.
- **Evolving stakeholder landscape & changing crisis landscape *(legal, organization)***: the presence of different stakeholders throughout the crisis creates the uncertainty of maintaining data management practices established during the response stage. Context also puts time pressure on data collection approach, mobilizing data management resources, establishing a data environment, and using standards and protocols.

## 7.1 Emergent nature

With the need for continuous adaptation to the emerging situation, organizations over time started developing more structural approaches, most notably moving from acquiring offered or available information to the acquisition of data based on identified information needs and gaps. This was due in part to more clearly defined objectives and requests received from partner organizations, which, among others, led to organizations to establish procedures and arrangements to exchange data with partners. Most notable were changes regarding data confidentiality and ownership, with more clear agreements established throughout the crisis regarding data access rights and the purpose of data usage. Technical developments encouraged shifting towards more machine readable, structured data types (e.g., JSON or CSV files). Spurred on by the development of dashboards and monitors fulfilling recurring information needs. These adaptations to the data management approach were required to facilitate this more purposeful, deliberate approach that led to more formal agreements and relationships with partners.

## 7.2 Diversity

The organizations, common in crisis response, constituted people with diverse backgrounds and expertise, each bringing their own perspective, networks, and relationships to the organization. At the same time, the organization faced pressure to deliver information and support to both policy makers and operational crisis responders. As one of the early members mentioned “We have to build the store while we are open for business.” These developments are not purely driven by the evolution of the organization but rather by the members of the organization. As the crisis evolved and the organization grew in size, and processes stabilized, members of the organization began looking for methods, tools, and options to reduce or more efficiently manage their workload. Nevertheless, the switch towards centralized systems and common procedures was challenging as over time information was stored on a range of different platform, using different approaches and classifications. Moving to a new central data management approach required additional capacity and resources. This development also introduced a more deliberate and structured approach towards IT-governance. While for technical aspects (such as backups and version control) the organization still relied on commercial solutions, other aspects were more explicitly managed. Security features such as access control were employed, and accounts (creation/deletion) was more carefully monitored. Likewise, general security audits were conducted.

## 7.3 Technical aspects

Constant influx of new technological advancements in various areas influence the technical considerations. As a result, across time, different technical solutions will be applied to different crises. It is for this reason that we argue that implications for data management are not so much in the realms of technical challenges since solutions will keep evolving to shift to the needs of organizations. Rather than focusing technological investments on developing specific

tools, policies, or systems, it is crucial to invest in capacities and capabilities that can be universally applied. The abilities to quickly identify, assess, and establish relationships with partners who can provide either data, analytical capacity, or data management support are key.

### 7.4 Stakeholder & Crisis landscape

All aspects of data management are affected by the nature of the crisis landscape. Increased time constraints, a general lack of resources, and a high level of ambiguity cause decision-makers to be under additional pressure to acquire, collect, store, and share data. Similar to how the need for adaptability within the organization affected data management practices, an evolving stakeholder landscape would impact those practices too. Due to the emergence of new stakeholders throughout the crisis, as well as the emergence of new information needs from existing stakeholders. The combination of these developments would change the data management requirements within the organization.

### 7.5 Practical implications

In a crisis situation, constrained time and resources influence the ability of organizations to implement data management procedures. Meanwhile, the context requires a continuous flow of high-quality information and thereby a well-structured, systematic approach to data management. To deal with this dilemma organizations should not only invest in 'data-preparedness' during the preparedness and recovery stage (so called 'cold-phase') but also need to realize that data management approaches require adaptability; a level of flexibility to respond to changing needs.

A practice worth considering is the development of data stewardship at both intra- and inter-organizational level (Wang et al., 2020). Data stewardship is the approach to realize the data management practices by having dedicated capacity to integrate these practices into the operational procedure. It is also an important mechanism to understand the scope, goal and needs of the data the institutions should acquire. Moreover, this dedicated capacity also ensures the interoperability of the data across different platforms (technically) and stakeholders (procedural and organizationally).

## 8. Conclusion

As the complexity of crisis situations is increasing, various advancements have led to an overall increase in the amount of data collected and used. At the same time data itself is an increasingly vital part of a *coordination* crisis response organization. As a coordinating body, rather than an operational agency or a policy maker, one of the main contributions to effective crisis response is the generation of information, and facilitating the data gather, analysis, and exchange. As more and more humanitarian actors have access to or possess data that can contribute to situational awareness, the potential of the data to crisis responders is rapidly growing. However, leveraging this potential comes with several challenges, as is clearly illustrated in the cases above. Whereas challenges would in the past be primarily technical in nature, most of them are less so today as advancements in standards, sharing platforms, and connectivity are adopted. Rather, challenges remain in the organizational aspects. Structuring the way data is made accessible therefore requires investing not just in novel technologies, but rather in data management processes and relationship-building.

### 8.1 Limitations & Future research

This paper presents the results of applying a framework to assess data management practices in two emergency response case studies. Future work would focus on further validating these findings through testing the framework on a higher number of crises, incorporating a variety of crises and crisis stages. Applying the framework beyond the realm of emergency response allows for a more comprehensive understanding of data management practices during crisis situations, as well as on how unique crisis characteristics influence the effectiveness of approaches. In particular, future research could consider inter-organizational networks and the role of information sharing in those networks, as now both case studies focused on data management practices within one organization. This is expected to add an additional layer of complexity to established organizational considerations as different considerations would be made across organizations. Especially for data governance, there is an opportunity for future work to assess how different governance considerations organizations take influence inter-organizational information sharing. A misalignment between organizations' data governance would be expected to obstruct the ability to share information effectively, but this connection has not yet been explored in crisis. Finally, we aim to explore in future research the crisis management lifecycle in relation to data management to see in more details how data management activities evolve over time. We acknowledge the impact of the people that constitute a crisis management response and especially the culture within the organization. Future research could investigate further the effect cultural characteristics have on the way data management is approached across different crises, as well as the effect it has on the effectiveness of data management. This would provide insight in the need for adaptable data management throughout crisis lifecycle. Adding the inter-organizational

aspect here would enable us to see the role of data management in the extent to which organizations share information across different phases of a crisis, a vital insight given the importance of inter-organizational coordination at each phase.

## 9. References


Al-Khouri, A. M. J. I. J. o. M., & Technology, I. (2012). Data ownership: who owns "my data". *2*(1), 1-8.

Ashish, N., Eguchi, R., Hegde, R., Huyck, C., Kalashnikov, D., Mehrotra, S., . . . Venkatasubramanian, N. (2008). Situational awareness technologies for disaster response. In *Terrorism informatics* (pp. 517-544): Springer.

Avison, D. E., Lau, F., Myers, M. D., & Nielsen, P. A. (1999). Action research. Communications of the ACM, 42(1), 94-97

Baharmand, H., Boersma, K., Meesters, K., Mulder, F., & Wolbers, J. (2016). A multidisciplinary perspective on supporting community disaster resilience in Nepal. *Proceedings of the International Conference on Information Systems for Crisis Resposne and Management, 12*.

Ball, A. (2012). *Review of data management lifecycle models*: University of Bath, IDMRC.

Bell, J., LaToza, T. D., Baldmitsi, F., & Stavrou, A. (2017). *Advancing open science with version control and blockchains.* Paper presented at the 2017 IEEE/ACM 12th International Workshop on Software Engineering Science

Brous, P., Janssen, M., & Vilminko-Heikkinen, R. (2016). *Coordinating decision-making in data management activities: a systematic review of data governance principles* International Conference Electronic Government

Buchanan-Smith, M., & Maxwell, S.. (1994). Linking relief and development: an introduction and overview. *25*(4), 2-16.

Chan, J., & Comes, T. J. P. E. (2014). Innovative research design–A journey into the information typhoon. *78*, 52-58.

Cheong, L. K., & Chang, V. J. A. p. (2007). The need for data governance: a case study. 100.

Clarke, R. J. I. S. J. (2016). Big data, big risks. *26*(1), 77-90.

Coombs, W. T. (2021). *Ongoing crisis communication: Planning, managing, and responding*: Sage Publications.

Coyle, D., & Meier, P. (2009). New technologies in emergencies and conflicts: The role of information and social networks. In *New Technologies in Emergencies and Conflicts: The Role of Information and Social Networks*: United Nations Foundation; Vodafone Foundation.

de Goyet, C.. (2008). Information gaps in relief, recovery, and reconstruction in the aftermath of natural disasters. 23.

Endsley, M. R. (2001). *Designing for situation awareness in complex systems.* Paper presented at the Proceedings of the Second International Workshop on symbiosis of humans, artifacts and environment.

Fitzgerald, A. J. e. A. (2009). Sharing environmental data: the role of an information policy framework and licensing. 1-2.

Kitchin, R., & society. (2014). Big Data, new epistemologies and paradigm shifts. *1*(1), 2053951714528481.

Kuiper, M. E., de Bruijn, A. L., Reinders Folmer, C., Olthuis, E., Brownlee, M., Kooistra, E. B., ... & Van Rooij, B. (2020). T*he intelligent lockdown: Compliance with COVID-19 mitigation measures in the Netherlands*. Amsterdam Law School Research Paper, (2020-20).

Lissenden, J., Maley, S., & Mehta, K. (2015). An era of Appropriate Technology: Evolutions, & opportunities. *3*(1).

Luokkala, P., & Virrantaus, K. J. S. s. (2014). *Developing information systems to support situational awareness and interaction in time-pressuring crisis situations. 63*, 191-203.

McConnell, A. J. P., & Society. (2011). S*uccess? Failure? Something in-between? A framework for evaluating crisis management. 30*(2), 63-76.

Meesters, K. (2021). Crisis Information Management: From Technological Potential to Societal Impact. *The New Common*, 153.

Meier, P. (2015). *Digital humanitarians: how big data is changing the face of humanitarian response*: Crc Press.

Meier, P. J. I. l. R. R. C. (2011). New information technologies and their impact on the humanitarian sector. *93*, 1239.

Quarantelli, E. L. (2005). *What is a disaster?: New answers to old questions*: Xlibris Corporation.

Reddy, M. C., Paul, S. A., Abraham, J., McNeese, M., DeFlitch, C., & Yen, J. J. I. j. o. m. i. (2009). Challenges to effective crisis management: using information and communication technologies to coordinate emergency medical services and emergency teams. *78*(4), 259-269.

Rodríguez, H., Quarantelli, E. L., Dynes, R. R., Andersson, W. A., Kennedy, P. A., & Ressler, E. (2007). *Handbook of disaster research* (Vol. 643): Springer.

Sharma, P., Joshi, A. J. J. o. H. L., & Management, S. C. (2019). Challenges of using big data for humanitarian relief: lessons from the literature.

Stahl, B. C., Wright, D. J. I. S., & Privacy. (2018). Ethics and privacy in AI and big data: Implementing responsible research and innovation. *16*(3), 26-33.

Van De Ven, J., van Rijk, R., Essens, P., & Frinking, E. (2008). *Network centric operations in crisis management.* Paper presented at the 5th International ISCRAM Conference, Washington, DC, USA.

van den Homberg, M., Meesters, K., & Van de Walle, B. (2014). Coordination and information management in the Haiyan response: Observations from the field. *78*, 49-51.

Wang, Y., & Meesters, K.(2020). Assessing Barriers in Information Sharing via Serious Games: A Case Study of DIMB. *European Conference on Games Based Learning*,

Wang, Y., Teperek, Marta, Andrews, Heather, Martinez Lavanchy, Paula, Ilamparuthi, Santosh, Turkyilmaz-van der Velden, Yasemin, & Plomp, Esther. (2020). Data Management Concept Note for General Public.

Wiles, R., Crow, G., Heath, S., & Charles, V. J. I. j. o. s. r. m. (2008). The management of confidentiality and anonymity in social research. *11*(5), 417-428.

Woods, D. D., Patterson, E. S., Roth, E. M. J. C., Technology, & Work. (2002). Can we ever escape from data overload? A cognitive systems diagnosis. *4*(1), 22-36.

Yin, R. K. (2012). Case study methods.

Yoon, V. Y., Aiken, P., & Guimaraes, T. J. I. R. M. J. (2000). Managing organizational data resources: quality dimensions. *13*(3), 5-13.