What is ‘Humanitarian Communication‘?

Towards Standard Definitions and Protections for the Humanitarian Use of ICTs

Nathaniel A. Raymond / Brittany L. Card / Ziad al Achkar

Introduction

Information communication technologies (ICTs) are increasingly becoming a defining component of twenty-first century humanitarian response operations during both natural disasters and armed conflict.[1] ICTs are employed in a variety of ways by non-governmental, governmental, and local communities and actors – a trend which is likely to continue with ever more complex implications for organisations and affected communities.

Some of the more prevalent uses of ICTs in humanitarian contexts by humanitarian organisations and affected populations include:

- Remotely collecting and analysing social media, geospatial data and other sources of data;[2]
- Communicating information in order to improve situational awareness and dispel rumours;[3] and
- Connecting affected populations to response activities.[4]

A report on the 2013 Typhoon Haiyan in the Philippines by the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) describes the increasingly important role of communication through the use of ICTs, stating:

> Aid organizations are increasingly recognizing and prioritizing communication as a form of assistance – one as important as water, food and shelter. Without access to information, disaster survivors cannot access the help they need or make informed decisions about their recovery...Disasters like Typhoon Haiyan, show that humanitarian actors are increasingly using communication tools – radio, mobile phones, social media – to access, communicate and disseminate information that may save lives or improve living conditions.[5]

However, there exists little or no accepted operational doctrine, nor precedents for applying traditional humanitarian principles to ICT-supported operations. This gap in pedagogy is an urgent issue given that both risks inherent to the humanitarian environment and direct threats to the human security of populations and organisations involved in this work are multiplying and transforming faster than the sector has adapted to face them.[6]

Humanitarian actors are increasingly required to assess and manage the negative impacts that these technologies may create and/or magnify, with little agreed guidance about how to do so. The goal of this paper is to frame three critical questions that may help to address the pedagogical gap facing the humanitarian sector in this area:

1. What should be the basis for defining ‘humanitarian communication’?
2. How do definitions of ‘humanitarian space’ need to change to include current humanitarian uses of ICTs?
3. How should internationally protected acts of ‘humanitarian communication’ be defined and by what standards are they protected?

[1] UNOCHA(2014). World Humanitarian Data and Trends 2014. Available from: http://www.unocha.org/data-and-trends-2014/downloads/World%20Humanitarian%20Data%20and%20Trends%202014.pdf [Accessed 23 September 2015].

[2] ‘Shamanth K. et al. (2011). TweetTracker: An Analysis Tool of Humanitarian and Disaster Relief. *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media.* Available from: http://www.public.asu.edu/~mabbasi2/papers/kumar2011tweettracker.pdf [Accessed 23 September 2015].

[3] Raymond, N. et al. (2013). While We Watched: Assessing the Impact of the Satellite Sentinel Project. *Georgetown Journal of International Affairs.* Available from: http://journal.georgetown.edu/while-we-watched-assessing-the-impact-of-the-satellite-sentinel-project-by-nathaniel-a-raymond-et-al/ [Accessed 23 September 2015].

[4] Internews (2013). Communication During Disasters: Examining the Relationship between Humanitarian Organizations and Local Media. Available from: http://www.internews.org/sites/default/files/resources/Internews_SIPA_communicating_disastes_2013-09.pdf [Accessed 23 September 2015].

[5] UNOCHA (2014). Philippines: Typhoon Haiyan and the Digital Last Mile. Available from: http://www.unocha.org/top-stories/all-stories/philippines-typhoon-haiyan-and-digital-last-mile. [Accessed 18 August 2015].

[6] Reilly, L. and Vazquez, R. (2015). Communications Technology: Challenges and Opportunities for Humanitarian Security. *WGET ICT Humanitarian Innovation Forum.* Available from: https://wget36.wordpress.com/2015/05/08/19/. [Accessed 18 August 2015].

Defining 'humanitarian communication'

The increasing use of ICTs by responding organisations and affected populations has changed how information is communicated and received during crises. It may even be changing how some crises occur and unfold. Yet, despite this transformative impact, there is no accepted definition of what constitutes 'humanitarian communication', nor what defines the 'humanitarian use of ICTs'.

Populations, principles and purposes

This paper proposes that three interdependent criteria must all be present simultaneously for communication activities, including the use of ICTs, to be considered truly humanitarian. These three 'P's' are populations, principles, and purposes. These terms are defined as follows:

- Populations: those engaging in communication, including the use of ICTs, are either the crisis-affected populations or organisations intending to assist affected populations as their primary goal;
- Principles: the actors and their activities must both uphold and comport with all four core humanitarian principles of humanity, impartiality, neutrality, and independence, as defined by Red Cross/NGO Code of Conduct;[7] and
- Purposes: the fundamental purpose of the communication activities must be 'to save lives, alleviate suffering and maintain and protect human dignity during and in the aftermath of man-made crises and natural disasters, as well as to prevent and strengthen preparedness for the occurrence of such situations'.[8]

Put together, the 'three Ps' provide the following definition of humanitarian communication:

> Humanitarian communication is technical capacity building; information collection and dissemination; preparedness activities; and/or data analysis for the purposes of saving lives, alleviating suffering, and protecting the dignity of crisis-affected populations when performed in accordance with international standards of humanity, impartiality, neutrality, and independence.

Challenges to agreeing a common definition of 'humanitarian' communication

Currently, ad hoc definitions and acceptance of what is considered humanitarian communication and use of ICTs is based primarily on two of the three above criteria: who is performing the action and for what purposes. This paper argues that defining communication activities as humanitarian, and thus as an internationally protected act of humanitarian assistance, depends on determining that all 'three Ps' are present.

As Raymond and Card contend, the application of humanitarian principles specific to the unique and challenging case of humanitarian communication has not yet been researched, let alone codified, to the point of being capable of routinely implementation.[9] Comprehensive doctrine to guide the execution of these activities in line with the core tenets of the Red Cross/NGO Code of Conduct is required for any ICT-supported activities to truly be humanitarian. The current approach of defining activities as humanitarian based only on 'people' and 'purposes' is insufficient.

Another major challenge to agreeing common definitions of humanitarian communication is that the individuals and organisations utilising technology for ostensibly humanitarian purposes are increasingly diverse and rapidly changing. Many fields of humanitarian response include heterogeneous groups of actors extending well beyond the individuals and agencies that have traditionally been considered as humanitarians.

Rather than being a temporary trend, this phenomenon is becoming a defining characteristic of the sector. Traditional humanitarian actors – such as NGOs and UN agencies – now actively partner with a mix of private corporations and voluntary technical organisations (VTOs) as a necessary step for accessing basic data and resources to do this type of work.

These newer actors and organisation types are often unfamiliar with traditional definitions and standards of 'humanitarianism'. In some cases, these newer actors in the 'humanitarian' ICT space actively eschew or challenge more orthodox concepts of what defines humanitarian aid. In this context, agreeing basic parameters for how to identify and evaluate the 'populations', 'purposes', and 'principles' involved in any ostensibly 'humanitarian communication' activity is a crucial step towards the development of any common doctrine.

[7] International Federation of Red Cross and Red Crescent (undated). Code of Conduct. Available from: www.ifrc.org/en/publications-and-reports/code-of-conduct/ [Accessed 18 August 2015].

[8] Global Humanitarian Assistance (undated). Defining Humanitarian Assistance. Available from: www.globalhumanitarianassistance.org/data-guides/defining-humanitarian-aid. [Accessed 18 August 2015].

[9] Raymond, N. and Card, B. (2015). Applying Humanitarian Principles to Current Uses of Information Communication Technologies: Gaps in Doctrine and Challenges to Practice. Available from: http://hhi.harvard.edu/sites/default/files/publications/signal_program_humanitarian_principles_white_paper.pdf. [Accessed 18 August 2015].

Defining 'humanitarian communications space'

At present, ICT-supported responses and civilian communication for humanitarian purposes can already be considered humanitarian assistance under any reasonable definition of 'humanitarian aid'.[10] Thus these activities, it can be argued, are already protected under current international legal prohibitions against disrupting humanitarian assistance and legal obligations to respect 'humanitarian space'.[11]

Traditionally, 'humanitarian space' is most often defined in terms of the physical and normative operational environment in which humanitarian agencies deliver assistance and interact with affected populations. However, robust debate exists about the precise definition of the term.[12]

The increasing integration of ICTs into the operational toolkits of traditional humanitarian actors, combined with the rapid adoption of ICTs by crisis-affected populations themselves, radically alters and expands accepted ideas of what constitutes 'humanitarian space'. In OCHA's 2014 paper, *Humanitarianism in the Age of Cyber-Warfare*, Daniel Gilman suggests that humanitarians should 'promote the idea of a "humanitarian cyberspace" [in which] humanitarian information systems should be off-limits for attacks'; humanitarians should 'advocate that in some cases cyber-attacks on humanitarian actors are violations of international humanitarian law.' [13]

However, Gilman's recommendation illuminates the underlying challenge of defining 'humanitarian communication space' in the digital age. Unlike other forms of traditional humanitarian assistance, humanitarian communication is very rarely explicitly addressed – if at all – under international law.

Additionally, defining 'humanitarian' cyberspace (or communication space) is also complicated by the fact that civil society, the private sector, and military actors often use the same data platforms and infrastructure. As a consequence, a legitimate attack on a network or data centre, in some cases, may simultaneously impact humanitarian providers and affected communities as well.[14]

Defining international protection standards for acts of 'humanitarian communication'

Defining 'humanitarian communication space' is contingent on first identifying which communication activities should be considered as protected and which as prohibited under international law. The five areas below are gaps within International Humanitarian Law, human rights standards, and/or codes of humanitarian practice. These gaps need to be addressed in order to define a protected 'humanitarian communication space'.

The five areas listed below have potential for the development of explicit protections and prohibitions related to 'humanitarian communication' and 'communication space'. The list is neither conclusive, nor exhaustive.

- **Prohibit the intentional targeting of civilians via ICTs**

The use of ICT devices, ICT-derived data, or other communications actions or platforms to specifically identify and target civilian populations for gross human rights abuses should be explicitly prohibited. Civilians should be able to freely transmit evidence of humanitarian crises and their effects as well as evidence of abuses (including, though not limited to, mass atrocities), and to freely send and receive information needed to migrate and/or receive assistance during humanitarian crises.

- **Protect the free flow of humanitarian information**

All crisis-affected populations have a right to engage in the free flow of humanitarian information to and from their community during crisis without either digital or analogue disruption or harassment. Communications shall not be intentionally targeted or disrupted to deprive affected populations of information about, or digital access to, humanitarian assistance.

- **Ensure communications access and capacity**

Governments and other actors in the communications space have a responsibility to reasonably facilitate the access and capacity of communities and humanitarian organisations to freely collect and share information relevant to response activities. Wilfully failing to

[10] Global Humanitarian Assistance (undated). Defining Humanitarian Assistance. Available from: http://www.globalhumanitarianassistance.org/data-guides/defining-humanitarian-aid. [Accessed 18 August 2015].
[11] Rottensteiner, C. (1999). The Denial of Humanitarian Assistance as a Crime under International Law. Available from: https://www.icrc.org/eng/resources/documents/misc/57jq32.htm. [Accessed 21 August 2015].
[12] ODI (2010). Humanitarian Space: Concept, Definitions and Uses Meeting Summary. Available from: http://www.odi.org/sites/odi.org.uk/files/odi-assets/events-documents/4648.pdf. [Accessed 18 August 2015].
[13] Gilman, D. (2014). Humanitarianism in the Age of Cyber-warfare: Towards the Principles and Secure Use of Information in Humanitarian Emergencies. *UN Office for the Coordination of Humanitarian Affairs*. Available from: https://docs.unocha.org/sites/dms/Documents/Humanitarianism%20in%20the%20Cyberwarfare%20Age%20-%20OCHA%20Policy%20Paper%2011.pdf. [Accessed 23 September 2015].
[14] Lin, H. (2012). Cyber conflict and international humanitarian law. *International Review of the Red Cross*, Volume 94, Number 886, Summer 2012. Available from: https://www.icrc.org/eng/assets/files/review/2012/irrc-886-lin.pdf [Accessed 23 September 2015].

provide crisis-affected populations with adequate and consistent access to communications infrastructure and services should be prohibited.

- **Protect response coordination**

All populations have the right to organise and coordinate – both internally and with outside actors – humanitarian operations related to emergencies affecting them or communities that they are connected to by race, religion, ethnicity, or other reason.

- **Prevent fraud and exploitation**

Governments and humanitarian actors have a responsibility to protect affected populations from fraud, exploitation, profiteering, and other activities attempting to either harm or benefit criminally from the circumstances, presence of aid resources, or potential vulnerabilities unique to crisis-affected populations.

Conclusion

Agreeing common definitions is the first step towards updating humanitarian doctrine to remain relevant and effective in the digital age. The advent of ICT-supported humanitarian response has so far focused largely on the potential benefits of integrating these technologies into traditional aid operations.

Affected communities, practitioners, governments, and the private sector, however, need clearer guidance to address challenges that new technology alone can't solve. When international law was first drafted, it could not have been imagined what an impact – both positive and negative – mobile devices, geospatial sensors, and the cloud would have on affected populations and providers.

It is time for the humanitarian community to revisit and revise the definitions of what constitutes 'humanitarian' aid in a networked world. As a result, we will be able to begin the long and iterative process of developing standards based on these definitions to protect technology's promise and help mitigate its perils.

European Interagency Security Forum (EISF)

EISF is an independent network of Security Focal Points who currently represent 75 Europe-based humanitarian NGOs operating internationally. EISF is committed to improving the security of relief operations and staff. It aims to increase safe access by humanitarian agencies to people affected by emergencies. Key to its work is the development of research and tools which promote awareness, preparedness and good practice.

EISF was created to establish a more prominent role for security risk management in international humanitarian operations. It facilitates exchange between member organisations and other bodies such as the UN, institutional donors, academic and research institutions, the private sector, and a broad range of international NGOs. EISF's vision is to become a global reference point for applied practice and collective knowledge, and key to its work is the development of practical research for security risk management in the humanitarian sector.

EISF is an independent entity currently funded by the US Office of Foreign Disaster Assistance (OFDA), the Swiss Agency for Development and Cooperation (SDC), the Department for International Development (DFID) and member contributions.

www.eisf.eu

About the Communications Technology and Security Risk Management Hub

The Communications Technology and Security Risk Management Hub is a project by EISF that was launched in October 2014. The project aims to begin a conversation towards a better understanding of the specific nature of the security threats created by the digital revolution, and the implications for the security risk management of humanitarian staff and programmes.

The first publication of this project (October 2014) brought together 17 authors who analysed in 11 articles how communications technology is changing the operational environment, the ways in which communications technology is creating new opportunities for humanitarian agencies to respond to emergencies, and the impact that new programmes have on how we manage security.

The hub aims to provide an outlet for researchers and practitioners to make original and policy-relevant research available to the humanitarian community. Each article is reviewed by at least two experts. If you would like to contribute please contact the editor of the series at eisf-research@eisf.eu.

http://commstech-hub.eisf.eu

Disclaimer

EISF is a member-led grouping and has no separate legal status under the laws of England and Wales or any other jurisdiction, and references to 'EISF' in this disclaimer shall mean the member agencies, observers and secretariat of EISF.

While EISF endeavours to ensure that the information in this document is correct, EISF does not warrant its accuracy and completeness. The information in this document is provided 'as is', without any conditions, warranties or other terms of any kind, and reliance upon any material or other information contained in this document shall be entirely at your own risk. Accordingly, to the maximum extent permitted by applicable law, EISF excludes all representations, warranties, conditions and other terms which, but for this legal notice, might have effect in relation to the information in this document. EISF shall not be liable for any kind of loss or damage whatsoever to you or a third party arising from reliance on the information contained in this document.