

Protecting Workers from Cyberbullying within Digital Humanitarian Response



May 2021



Licensing Information

“Protecting Workers from Cyberbullying
within Digital Humanitarian Response”
by Batool Barody and Andrej Verity
is licensed under Creative Commons
Attribution-NonCommercial 3.0 Unported.



Protecting Workers from Cyberbullying within Digital Humanitarian Response



By

Batool Barody (batool.barodi@mail.utoronto.ca | [@batoolbarody](https://twitter.com/batoolbarody))

Master of Global Affairs

Munk School of Global Affairs and Public Policy, University of Toronto

Andrej Verity (verity@un.org | [@andrejverity](https://twitter.com/andrejverity))

United Nations Office for the Coordination of Humanitarian Affairs (OCHA)

Design

Lorena Velázquez (lorena.velazquezsanjose@un.org | kunoichidesign.com)

United Nations Office for the Coordination of Humanitarian Affairs (OCHA)

This document was made possible with the support of



OCHA

Table of Contents



05	Executive Summary
05	Overview of Cyberbullying and Harassment
07	Different Types of Cyberbullying
08	Liabilities and the Role of International Organizations in Creating a Bullying-Free Environment
09	Recommendations
12	Conclusion

Executive Summary



The Internet, particularly social media, has expanded the frontiers of bullying and harassment in workplaces and educational institutions. This brings a host of issues for employees, including those working in the digital humanitarian response field.¹ This paper outlines the varying definitions of cyberbullying; provides an overview of the evolving landscape; reviews recent cases relating to the responsibility of employers and online platforms; and outlines strategies to inform users how to respond to and protect themselves from cyberbullying.

This paper aims to serve as practical guidance for people or organizations who create, manage or support digital communities that respond to emergencies. The goal is to empower those responding to emergencies digitally and make their environment free of cyberbullying.

Overview of Cyberbullying and Harassment



The advances in technology and social media have changed the world in many positive ways, but they have also had negative side effects, which include the emerging type of harassment called cyberbullying.

Cyberbullying is the use of information and communications technology to harass and harm in a deliberate, repetitive and hostile manner.² It can take many forms, including bullying through social media, harassment, sexting, cyberstalking, deception, impersonation and sending nasty messages via chat rooms and instant messenger.³ Cyberbullying follows many of the underlying dynamics of more traditional forms of bullying, but it features some unique qualities that can magnify the damage caused and make it more difficult to detect.

Given the particular nature of cyberbullying and the growing number of variations resulting from rapid technological developments, cyberbullying creates a unique group of victims who may need special treatment. The increasing pervasive nature of technology in our modern society is only expected to exaggerate the challenge.

The problems related to cybersecurity and cyberbullying are increasingly evident and prejudicial to workers and volunteers in the field of humanitarian response worldwide, regardless of their race, age, religion or sexual orientation. The negative and psychological

¹ Standing Senate Committee on Human Rights, (2012). “Cyberbullying Hurts: Respect for Rights in the Digital Age” available online at: <http://sencanada.ca/Content/SEN/Committee/411/ridr/rep/rep09dec12-e.pdf>

² Stopbullying.gov, 2014

³ Notar C. E., Padgett S., and Roden J. (2013). Cyberbullying: Resources for Intervention and Prevention. *Universal Journal of Educational Research* 1(3), pg. 133. DOI: 10.13189/ujer.2013.010301

impacts of cyberbullying are taking their toll on individuals, society's overall health, the education system and basic social services, among others. These impacts have led to changes in international organizations' human resources-related policies when it comes to dealing with extreme weather events and anthropogenic disasters worldwide. The COVID-19 pandemic has pushed these issues and changes to the forefront.

In the field of cyberbullying related to humanitarian emergencies, social scientists have explored areas such as cyberbullying risk factors;⁴ the personalities of actors, victims, bullies, and bystanders involved in cyberbullying;⁵ and workers' views towards cyberbullying.⁶ Meanwhile, computer scientists have focused on developing automated approaches for cyberbullying detection using text mining and data. Research studies specific to social media platforms, such as Twitter, have included characterizing hashtags associated with bullying,⁷ detecting cyberbullying messages through feature selection⁸ and conducting a language-specificity analysis, as carried out on Twitter to discover Indonesian bullying patterns.⁹

It can be challenging to make ethically justified decisions in humanitarian emergencies – whether in-person or remote. Given that cyberbullying exists predominantly in digital humanitarian aid response groups (versus in-person responders), it can become even more challenging to promote values such as impartiality, well-being and coherence among digital workers and volunteers.



“Cyberbullying is incredibly effective; it is one of the reasons I am no longer in this space.”



Interviewee

4 Anderson, Bresnahan & Musatics, 2014; Jung et al., 2014; Peskin, 2014; Sampasa-Kanyinga, Roumeliotis, & Xu, 2014

5 Camacho, Hassanein, & Head, 2014; Lohman, 2015

6 Eden, Heiman, & Olenik-Shemesh, 2013; Moreno & Kota, 2014

7 Calvin, Bellmore, Xu, & Zhu, 2014

8 Nalini & Sheela, 2015

9 Margono, Yi, & Raikundalia, 2014

Different Types of Cyberbullying



Creating a safe environment for workers and volunteers will ensure a team is robust, respected, and ready to provide the necessary help under stressful circumstances. To create effective solutions, it is important to analyse the two different types of cyberbullying.

The first type occurs in the immediate response phase, when everyone is rushing to get things set up. The bully “takes over” the project and issues demands or commands, even though they are not authorized to do so, or they make excessive demands on volunteers. In this type of situation, digital responders often do what the bully dictates because it is an emergency and/or they do not have extensive experience within the group, thus not realizing that the bully is out of line.

The second type occurs when the bully has been with an organization for some time. This causes them to feel they know better than not just the other responders, but the group members who may be legitimately in charge of a project. The bully feels they are in charge even though they are not, making them possessive of the project and the group. Thus, they may deliberately contradict those in charge, causing confusion and problems for other project members as the chain of command becomes unclear. Moreover, they may not listen to the project leaders and may talk down to project members. Generally, this type of bully considers themselves as being helpful, and they do not feel they are doing anything wrong or malicious. But not listening to the project manager results in the need for a more senior official to step in and inform the bully that s/he is out of line.

This type of bully will not be appeased and generally ends up quitting the project/organization.¹⁰ This type of bully tends to be much more common in volunteer-based organizations, especially groups that have long-time members and those who have more time to spend on the organization.

¹⁰ Weisberg-Ross R. (2010). The Basics of Bullying and How to Stop It. Good Therapy. www.goodtherapy.org/blog/adult-bullies/

Liabilities and the Role of International Organizations in Creating a Bullying-Free Environment



Rapid technological change has blurred the boundaries between personal and workspace-related affairs. Therefore, employers are challenged with having to develop guidelines and policies that direct the appropriate use of technology and maintain a civil workplace. Due to the lack of a shared understanding around the issue of cyberbullying, it will be challenging to develop binding international legislation. The challenge is exacerbated because of the rapid change in the capabilities of technology, the diverse social norms about technology's use, and the uncertainty of the role and responsibility of employers in minimizing cyberbullying and facilitating a civil workplace environment.

Many countries have a national anti-bullying law, but not all countries have policies enforcing that law. For this reason, not every company and incident are held to the same standard. Furthermore, when it comes to international humanitarian organizations, cyberbullying and related behaviours are treated differently in every country and organization due to a lack of international law.

Employers and managers should make it known that digital discrimination and cyberbullying will not be tolerated, regardless of whether or not an international law is in place, and employees should be made aware of impending consequences.



Recommendations



This section provides **six concrete actions** that organizations and digital humanitarian response teams can take to protect their employees and volunteers from cyberbullying when responding remotely to humanitarian emergencies.

1

Put welfare and professionalism at the heart of any group

To create a cybersafe environment during emergencies, the most important recommendation is to have a dedicated focal point or team within the responding group who can handle problematic behaviour effectively. All members should be made aware of this role. The focal point or team must remain an objective observer so that group members will view them as impartial and be willing to approach them with issues or complaints.

To prevent cyberbullying, the systems in place for dealing with conflicts and bullying must be up and running, with no interruptions, and all members must know about them before emergencies. The midst of an emergency is not the time to be figuring things out. Plans need to be formalized in advance in order to train all members on the conflict-resolution system and to ensure that any new member learns about the system during onboarding. If a reliable system exists, members will use it if they know about it. Preparation is the key to preventing digital discrimination and creating safer teams. As Brodsky explained:

“To create a safe environment, whatever system is in place for handling conflicts and bullying must be set up and running smoothly and all volunteers should know about it prior to emergencies.”

Jae Brodsky

The Former Vice-Chair of Statistics Without Borders

It is also important to apply the concept of professionalism directly into the description of the services of digital response entities. When members know that there is an expected level of professional behaviour, project managers undergo more extensive training and become more comfortable with asking for help if a member behaves inappropriately. Professionalism helps to identify when someone is a subject-matter expert for a given project, thereby enabling the entity to define such roles and responsibilities in advance. This preparation reduces the number of conflicts that can occur between project members.

2

Develop or customize appropriate policies

It is vital to ensure that appropriate policies are in place. These can be policies dedicated to cyberbullying or adjustments to existing ones. Another important policy or standard operating procedure could be related to the consent of information movement of responders and the affected population so that people understand where, when and what data can move.

Making it clear to members that an organization takes such topics seriously can have an extremely positive effect on a group's morale. It can also decrease the amount of potential conflict and/or serious consequences, thereby deterring one member from bullying others.

Looking more globally, if an organization can frame international authoritarian language that could be applied to all digital response groups, it could bring more uniformity across organizations and geographical boundaries.

3

Avoid politics

Ask members to avoid political conversations, whenever possible. Friendly reminders of the group's core mission can help members steer the topic back to a constructive response.

4

Provide training

Managers are critical in setting the group's tone and identifying and resolving issues. Managing and coordinating from a distance is particularly challenging and thus requires specific skills. Training should focus broadly on managing remotely, motivating group members and being approachable. Role modelling and good online behaviour are important. Managers need to be aware that receiving a barrage of emails or Slack messages outside working hours can be stressful or even distressing for members, creating a sense of pressure. A manager must be able to spot warning signs, which can be very challenging to do when team members are not physically present. Being virtual makes it more important than ever for managers to have the skills and tools to notice when workers are struggling, withdrawing or being ostracized from the team.

Employers, or umbrella organizations, need to proactively prevent cyberbullying by implementing training and policies for staff and volunteers. This action will help educate people on how to recognize and respond to potential attacks as well as provide procedures and resources for those affected.

5

Foster the right culture and encourage record-keeping

Setting a strong and respectful culture within the organization around harassment being unacceptable is imperative. So is having clear and transparent processes for escalating misbehaviour. These could range from a code of conduct to an ethics hotline, but it will depend on the nature and size of the organization. It is important to have these practices in place so that harassment from inside the organization is mitigated in a timely fashion.

Implementing a third-party, anonymous reporting channel and training members how to use it will give them the outlet to report a problem when they are not comfortable going to their manager or team leader. This anonymity helps create a safe environment and gives members a way to report cyberbullying incidents without being ignored or discriminated against.

When a negative incident occurs, it is strongly advised to retain details for a set minimum number of months. Although some organizations may face budgetary constraints, it is recommended that details are kept for an absolute minimum of three months. Retention should align with details outlined in any harassment-related policies. If the tools in use have restrictive measures (e.g. free accounts on Slack retain content only for a short period), group members should be advised to take screenshots of inappropriate messages they receive and immediately report this to the relevant department.

6

Develop strategic partnerships

Finding the right partners for humanitarian response can provide a positive, compounding effect. These could be partnerships that augment the on-the-ground response or ones in which the new organization becomes a dedicated welfare support group.

Even technological companies can help digital response groups. They can help directly by exposing sensitive information carefully (e.g. requiring an extra click to see traumatic photos). They can also help at a more personal level. For example, Google blurs conflict areas so that people do not zoom in and accidentally see traumatic material. Such censorship can also help deter unscrupulous actors.

Conclusion



Cyberbullying is an unfortunate reality of our twenty-first century, online world, and those in the humanitarian disaster response arena are not immune to it. The literature review and the interviewees made it clear that the topic will only become more and more critical over time.

Technology continues to change rapidly, and cyberbullying techniques continue to adjust. Therefore, it is critical for entities, formal or informal, to take concrete steps in dealing with the issue. Implementing the above recommendations will help to protect staff and volunteers, help to build a constructive and safe place where people want to work, and help enable a team that can aid the overall response and thus the people who are directly affected.

