ESRC Wales Doctoral Training Partnership
Partneriaeth Hyfforddiant Doethurol Cymru ESRC

Challenges in the digital age to humanitarian NGOs' functionality and legitimacy as global governance actors

Project description

How do cybersecurity and data protection challenges affect humanitarian NGOs' functioning and legitimacy in the global governance of humanitarian crises?

Humanitarian NGOs are increasingly influenced by digital data and, to retain a competitive edge in the global marketplace of aid, are forced to engage with audiences, donors, project partners and other stakeholders in cyberspace. Yet, as digital data collection increases within NGOs, so does the interest from antagonistic non-/state actors, who try to undermine NGO operations by exploiting existing vulnerabilities in NGO data security provisions. At the lower end of the spectrum, successful attacks from these threat actors can affect an NGO's brand; yet, rendering data vulnerable and exploitable can also result in severe consequences such as the revealing of personal identities and/or locations, and such instances have resulted in fatal attacks in the physical world.

Explorative talks with humanitarian NGOs show that many are ill-prepared to respond to cybersecurity and data protection threats. This jeopardises not only the credibility of their claim to 'do no harm', but their lack of vigilance arguably plays directly into the hands of those who seek to cause chaos to as many people as possible, and in many cases to physically harm 'easy targets' – aid workers and beneficiaries. This raises fundamental questions about the continuing suitability of 'neutrality' and 'impartiality' as core characteristics of any NGO response to a global crisis. Drawing on insights and concepts from fields such as International Relations, STS, Communication Studies, Computer Science and Law, this project makes a significant contribution to scholarship on humanitarianism by exploring how humanitarian NGOs are affected by data protection issues in their immediate work, and by theorising what this means regarding their capacity to address humanitarian crises.

The project takes a predominantly qualitative approach (e.g., document analysis, surveys, interviews, ethnographic observation) with humanitarian NGOs in the UK, the US and the Middle East, to investigate sub-questions such as:

- How do humanitarian NGO employees/volunteers understand the cyber threat landscape, and how do they weigh threats against the exigencies of the global marketplace of humanitarian aid?
- Which data security mechanisms do NGOs use, in what context, how, and what are the challenges? How have (a lack of) data-security practices affected NGOs' work and mission?
- What do the effects of the digital age on the work and legitimacy of humanitarian NGOs mean for the politics of international humanitarianism and global crisis governance?

Organisational partner

The project will be developed in collaboration with *Nonviolent Peaceforce*, an international nongovernmental organisation (INGO) whose mission is to protect civilians in violent conflicts through unarmed strategies. For more details, see https://www.nonviolentpeaceforce.org.

Main supervisor

The project's main supervisor is Dr Bliesemann de Guevara. She is a Reader in International Politics with a specialisation in conflict and intervention and the Director of the Centre for the International Politics of Knowledge. She leads several funded projects relating to violent conflict zones and has been collaborating with the project's partner organisation, Nonviolent Peaceforce, in a project on conflict knowledge in Myanmar and as a facilitator for a series of 'Good Practices in Unarmed Civilian-to-Civilian Protection' workshops in different world regions, which have raised the urgency of considering cyber security and data protection for international NGOs in political emergencies.