TECHPOPS

zif Center for International Peace Operations

100 Voices on Technology & Peace Operations

Ensuring adequate data handling, protection, usage, sharing and storage in peace operations

The hope and the hype - humanitarian protection in the digital space

20 December 2021 | Delphine van Solinge

> *"A problem not fully understood is unsolvable, and a problem that is fully understood is half solved."*
> *Charles Kettering*

Despite the many steps taken at regulatory and policy level to limit human suffering during war, civilians living in conflict zones and violent environments remain the principal victims of abuses and of the effects of violence. This reality is unfortunately showing no sign of abating. Some of the factors fueling violence include rivalrous dynamics[1], protracted ethnic, religious and sectarian tensions, weak rule of law, unequal access to resources, poverty and the impact of climate change, to name a few. In addition to these underlying drivers, the role of exponential digital technology, that is technology that grows and improves exponentially, should be looked at closely.

Humanitarian organizations, such as the International Committee of Red Cross (ICRC), work relentlessly toward ensuring the protection of the lives and dignity of victims of armed conflict and other situations of violence and to prevent human suffering. Although conflicts and related humanitarian harms are still manifesting primarily in the physical world, recent technological developments have introduced new layers of complexity to the way conflicts and violence play out and the way in which they may adversely affect the lives and safety of civilian populations on the ground.

"Protecting people" is at the heart of the ICRC's mandate. It is a complex area of work that must constantly adapt to evolving realities. This has led to new activities, as well as continuous reflections and engagement on the development and application of international humanitarian law (IHL), humanitarian policies and programs, and operational standards. Understanding new digital challenges and their different implications is therefore critical for the ICRC and humanitarian protection responders, as they begin to devise ways to address these challenges.

DIGITAL RISKS: WHAT HAVE WE OBSERVED?

While digital technologies can help improve the lives of individuals and communities affected by war and violence, depending on their uses they can also create additional and dire risks. Technological advances have enabled new means and methods of warfare, such as cyber-attacks, which today can disrupt or compromise critical infrastructure in countries at war remotely and anonymously. Cyber warfare between parties to a conflict[2] has been enhanced due to technology. Such advancements include the pace and reach of information that allow parties to a conflict to influence opinions, emotions and behavior at a large scale. Think for example about a rivalry between two parties who are putting up a single billboard in the city that can influence the perception and behavior of about a thousand people. And now think about the same two groups using social media's ability to influence billions of individuals across the world through attention harvesting and directing economy while driving each click and influencing people's behavior.

The spread of harmful content in the form of misinformation, disinformation and hate speech (MDH) on social media, which has featured quite heavily in recent crisis around the world, is a case in-point showing how technology can amplify risks for the people but also humanitarian organisations who try to serve them. Recent history has seen conflict situations during which Rights groups observed an important rise in social media posts inciting violence against ethnic minorities and encouraging civilians to take up arms. Polarizing and false content has been circulated widely on social media, inflaming ethnic tensions and violence between communities. In some instances, some humanitarian organisations have also been suspected or at worst suspended on account of spreading misinformation.

Artificial intelligence can be used for various purposes and functions such as predictive analytics, assessment and monitoring, or supply chain management. At the same time, it also raises questions due to the bias it inevitably carries and its impact on people as it for example replicate patterns of discrimination and stigma in automate decision-making processes (education, salary, job interview etc). The role that artificial intelligence and algorithms can play in spreading harmful content online and creating echo chambers is increasingly discussed and exposed in the public realm. The algorithms and machine learning models used by social media are designed to maximize time online and engagement which generate profit through increased advertisement exposure and clickbait. And human engagement is often best secured by showing polarizing content that taps into deep emotions such as disgust, fear and anger.

Another related exponential risk is the use and misuse of (personal) data which is collected on a massive scale by "surfing on the internet and social media" where we unwittingly giving away a lot of information about ourselves. Many of our lives will not necessarily be affected in dramatic ways; for people living in conflict areas, the story can be very different as vulnerability levels are higher and coping and resilience mechanisms often much weakened. People's personal information if misused may lead to protection concerns such as discrimination, forced displacement, persecution, detention etc.

100 Voices on Technology & Peace Operations

In recent years, increased concern has been voiced about the safety of affected populations and individuals whose personal information could lead to them being identified and tracked by certain actors through their digital histories and social media connections. Humanitarian organisations may contribute to those risks as they seek to try out innovative responses and technologies such as cashless programs or biometrics registration of people in already fragile contexts. Technologies are increasingly being used with the hope to enhance the efficiency and scale of humanitarian responses. However, this is often done with a techno-solutionism (not to mention techno-colonialism) approach and with limited understanding of the technology used and of the risks for affected people.

WHAT DOES IT MEAN IN TERMS OF HUMANITARIAN PROTECTION?

Based on the foregoing, one can infer two things. First, digital technologies, depending on their uses, can lead to real protection or safety concerns, with grave humanitarian consequences[3]. These may include for example both off-line and online stigmatization, discrimination, denial of access to essential services, surveillance, persecution, and attacks on the physical and psychological integrity of affected populations. Second, our lives and what happens in them is no longer limited to the physical environment we live in. Increasingly, what is happening online has repercussions offline and vice versa. As humanitarian protection practitioners, we need to be present on both fronts, but the question is how to do this and what it means to provide humanitarian protection in the digital space?

At this stage, there is not a clear answer to this but there are some elements to guide our reflection.

The growing use of digital technologies and data increases the need for enhanced data protection rights and safeguards to ensure the protection and dignity of people at risk, and the impartiality of humanitarian action. It is about moving from theory to practice. In other words, humanitarian organizations need to learn and understand how to responsibly use digital technologies and process digital data. This includes understanding the consequences by questioning whether digital tools that may expose people's safety in one way or another are the right solutions to their problems and, if so, how to mitigate risks at different levels. This requires investment and training that should not be overlooked but rather prioritized including by supporting organizations with more limited means.

Digital technologies have also introduced new types of actors in the ecosystem of conflicts, such as big tech companies, other private sector actors, hackers etc. Humanitarian organizations need to move beyond the tech hype and learn to engage both with traditional actors in armed conflict and new ones about the risks of deploying new technologies in armed conflict, the potential consequences on people, and the corresponding responsibility to mitigate the harms. Such engagement needs to be reflecting the changing nature of conflict and 'battlefields' as well as ways ensure accountability in the digital space.

100 Voices on Technology & Peace Operations

To deliver meaningful humanitarian protection work, it is critical to understand the vulnerabilities and risks people are facing and devise means to address them. As those vulnerabilities and risks also play out in the digital space, humanitarian organizations need to develop their capacity and skills, working closely with affected people and in partnership with academia, to detect and analyse these risks and assess how they affect the safety and dignity of the populations they are meant to serve. At the heart of these problems is the need for good techno-humanitarian analysis but above all, a clear commitment to a Neutral Impartial, Independent Humanitarian Approach (NIIHA) that can guide the sector toward better designs and more efficient responses with affected people.

In today's world, the greater the exponential power and technology, the more exponential risk is potentially created for the people, in particular those who find themselves in a vulnerable situation, such as an armed conflict. Defining what protection is in the digital space and how to deliver it, is an area that urgently needs attention if we want to remain relevant in the design and delivery of our humanitarian endeavor.

My hope is that this discussion and work will help decision-makers—from individual organizations to policy leaders—recognize hype, evaluate the humanitarian impact of emerging technologies in more realistic ways, and invest in developing standards to deliver humanitarian protection in the digital space.

FOOTNOTES

[1] In particular between great powers who avoid direct confrontations and use proxy countries to set their scores.

[2] Information warfare is as old as warfare itself. Military scholars consider that the use of information as a tactic in warfare would go back to fifth-century BC.

[3] Humanitarian consequences is understood here as the harm or suffering derived from the action or negligence of an authority, international and/or private entity, individual, community. It can be defined as any injury, loss or damage either material or intangible that impacts negatively on the basic needs, wellbeing and security of individuals or communities.

ABOUT THE AUTHOR

Delphine van Solinge is working at International Committee of the Red Cross (ICRC) as adviser on digital risks for populations in armed conflicts. She previously worked as Protection Coordinator in Chad, the Philippines, Afghanistan and Colombia and as Head of Unit for Global Protection Affairs in Geneva.