Nonviolent Peaceforce

UCP IN A DIGITAL AGE

Addressing Threats, Leveraging Tech for Protection

Introduction

Digital technologies are reshaping conflict and protection landscapes, introducing both unprecedented threats—such as doxxing of human rights defenders, AI-driven disinformation, and algorithmic biases—and requiring innovations and adaptations to protection responses. As technologies evolve, nonviolent strategies can be used to disrupt and prevent violence and protect civilians. Unarmed Civilian Protection (UCP) practitioners are actively identifying risks and leveraging digital tools to amplify proactive, civilian-centered protection strategies and to reduce violence.

Online-Offline Protection Risks and Responses

UCP centres the capacity of civilians to protect themselves and their communities when affected by violent conflict. This includes the identification of risks to civilians and developing strategies to address these risks. The protection risks posed by digital technology are numerous and new risks are likely to emerge as technologies evolve. Specific emerging threats to civilian safety related to digital technology include, but are not limited to, the following:

- The rapid spread of disinformation, misinformation, hate speech, and dangerous speech online can escalate violence offline (and vice versa). Communities affected by conflict have long used rumor control as a protection strategy, and this practice has expanded to online-offline spaces. These actions go beyond "fact-checkers" or online verification services to intervene to prevent the harmful escalation of dangerous speech before it leads to violence. For example, false images of a burning place of worship in one area could quickly incite interreligious tensions and retributive violence in cities located hours away. In response, UCP practitioners work to recognise such emerging disinformation (was this an AI-augmented image? an old image?), engage communities in de-escalation (through actions such as activating local leaders, engaging stakeholders in dialogue), and prevent violence longer-term through community education on recognising dangerous speech[1] and social cohesion strategies.

- Technology-Facilitated Gender-Based Violence (TFGBV) is a growing threat that extends violence into digital spaces, often serving as a precursor to real-world physical, sexual, and emotional violence. Women and LGBTQ+ individuals are frequently targeted through harassment, doxxing, and cyberstalking that can often lead to further offline violence. For example, image-based sexual abuse – where perpetrators obtain, share, or threaten to share compromising images without consent, using these threats to force compliance from those they target – can lead to suicide, physical and sexual abuse, and exclusion. Addressing such threats requires proactive, community-driven digital safety strategies that integrate protection into everyday online interactions. For example, in the Philippines, youth groups Titayan and CABCEP have developed Kadtag Magungaya, a program that trains young people, parents, and guardians to recognize and counter online sexual exploitation of children (OSEC) and other forms of cyber violence. This initiative equips communities with critical digital safety skills, helping them navigate and mitigate online threats. Scaling such models is essential to addressing TFGBV at its root, ensuring that digital protection remains embedded in broader UCP strategies.

1 PeaceTech Lab's Hate Speech Lexicon provides one model for how communities can track and mitigate harmful narratives.

- Digital technologies present additional threats to the security of sensitive information, which particularly poses risks to at-risk communities whose visibility—whether as human rights defenders or due to their identities—makes them targets. Especially in high-surveillance environments, digital threats such as data breaches, cyber espionage, and targeted attacks endanger both individuals and communities. Strengthening secure communication and data protection strategies is therefore critical to keeping people safe amid the risks posed by surveillance and cyber threats. For example, in South Sudan, NP provides continuous training on encryption, secure communication methods, and risk mitigation strategies for local partners handling sensitive data. Scaling such initiatives is vital to ensuring civilian protection in an era of increasing digital repression.

- Technology can be a tool, not a replacement, in civilian protection. Relying too much on technology like surveillance and remote monitoring can overshadow and obscure the views and experiences of civilians. While new technologies have made it easier to gather information from hard-to-reach places and provide more data for analysis, they cannot replace the important knowledge and perspective of people living through conflict. Mistakes in technology design can lead to incorrect risk assessments, and online alerts still need to be turned into practical safety measures. Instead of depending mainly on technology, UCP practitioners focus on sharing information in ways that put civilians and their communities at the center, using digital tools to support not replace these connections.

- Exacerbating existing inequalities. Disparities in access to technology, digital literacy gaps, and algorithmic create new protection risks and expand existing risks for marginalised communities. Differing access to technology keeps many civilians from resources, information and connections that can be vital to their safety. Similarly, a lack of knowledge on digital hygiene and digital literacy can expose civilians to increased targeting, harassment, and violence based on information they share or store in digital spaces. Algorithmic biases also contribute to increased identity-based marginalization as the experiences of those without a strong online presence are often underrepresented and not taken into account in online models. Finally, the widespread use of internet disruption as a tool of repression or warfare emphasizes the need to avoid overreliance on digital communication.

Youth workshop on Digital Citizenship. Maguindanao. 2023. ©Denise Rafaeli Cadorniga/NP

Enhancing Protection Through Digital Technologies

In response to these risks, UCP practitioners and local communities are integrating technology and digital strategies into their protection and safety planning and responses. Digital threats are multiplying, and these same technologies can strengthen protection efforts when grounded in community-led strategies. UCP practitioners have strategically employed digital technologies in creative and effective interventions throughout the globe.

- Either in lieu of or in addition to physical protective accompaniment of civilians, UCP actors can use digital tools to provide "digital accompaniment": remote monitoring and verification, check-ins, and virtual witness presence for at-risk individuals. Disability justice organizers such as Mia Mingus, Alice Wong, and Sandy Ho have led the way in using digital tools to expand access to safety, demonstrating how technology can be leveraged for protection. This approach has also offered critical protection in contexts ranging from civic engagement actions to civilian evacuations in humanitarian emergencies.

- There are many opportunities for EWER mechanisms to expand through the use of digital technology. Remote monitoring of satellite imagery, social media feeds, and other digital tools can provide information about imminent violent action, providing civilians with increased time to respond. For example, NP's Ukraine program is working to equip local partners with Frequency Analyzers that can help detect drone attacks, allowing frontline humanitarians to adapt their movements based on this information. Likewise, EWER volunteers in Myanmar are able to share information through digital networks, improving their ability to support civilian evacuations through triangulation with outside information.

Case Study: Digital Accompaniment in Crisis

When civil war erupted in Sudan, one NP staff member—Nina*—was visiting her family outside the country for Ramadan. Suddenly unable to return, she became a lifeline for the people she had met during her time working in Darfur. Through her phone, Nina stayed in touch with dozens of civilians attempting to flee. She checked in constantly, asking how they were doing, offering encouragement, and helping them navigate evacuation routes. On the ground, the situation was chaotic. Different exit points opened and closed unpredictably. Word began to spread that Nina had up-to-date information—sometimes relayed by families with patchy phone service—and people began sharing her contact. She became a digital accompanier, confirming which routes were open and which crossings had closed. Even when she couldn't guarantee safety, her messages offered clarity, connection, and critical psychosocial support. Civilians knew someone was looking out for them—even from afar.

- Digital technologies offer powerful tools to enhance peacebuilding efforts and civilian protection, not only by addressing the root causes of conflict but also by fostering connection and resilience in divided societies. In the Philippines, youth-led initiatives leverage online platforms to counter cycles of violence with narratives of peace, using digital spaces to challenge harmful rhetoric and promote social cohesion. During the Covid-19 pandemic, digital technologies allowed communities to remain connected and valuable peacebuilding efforts to continue. These examples highlight the potential of digital technology to reinforce localized, community-driven peacebuilding and protection strategies —when implemented with a principled, conflict-sensitive approach.

Advocating for Safer Digital Spaces

Ensuring a safer digital future requires systemic change—from internet governance to digital platform design to localized initiatives that strengthen community resilience. Advocacy plays a critical role in pushing for these changes - whether by demanding that platforms adopt pro-social design to reduce harm or by supporting grassroots efforts that equip communities with the tools to navigate digital threats. Without intentional action, digital technologies will continue to be shaped by structures that prioritize capital gain over safety, leaving civilians vulnerable to exploitation, disinformation, and violence. By advocating for digital spaces that center protection, transparency, and accountability, we can build a more secure future for all.

For example, digital peacebuilding leaders are pushing for platforms to adopt pro-social design —structuring digital spaces in ways that foster community and social cohesion while reducing the risks of violence and harm. These efforts emphasize the role of platform design in shaping safer digital environments, recognizing that structural choices influence how conflicts escalate or de-escalate online. UCP practitioners also play a key role in advocating for civilian-led protection efforts to be recognized in digital policy discussions. By ensuring that the experiences and expertise of at-risk communities inform policy decisions, they help shape digital spaces that prioritize safety, accountability, and inclusion.

Case Study: Confronting Digital Extortion

In South Mosul, Iraq NP and Community Peace Teams (CPTs) have engaged with local authorities to highlight crucial gaps in the decentralisation of digital extortion cases to local courts, making reporting more accessible and advocated for measures that ensure sensitive cases are handled with care. This advocacy is combined with protective accompaniment to increase survivors' access to National Security Services (NSS) and community-led initiatives to enhance local resilience by raising awareness about digital extortion and addressing barriers to reporting. These forums open dialogue between community members and duty bearers, resulting in increased responsiveness from security actors and empowering survivors to take action.

Discussion about online extortion issues between women from the community, women peace team, and community police, South Mosul. © NP

Recommendations

1. Regularly re-evaluate digital technologies recognising emerging protection risks and opportunities and adapting programming accordingly.

2. Consistently monitor protection threats facilitated by digital technology, working alongside communities to address these threats in digital and analog manners.

3. Continue to prioritise the experience and analysis of civilians most affected by violent conflict, using digital technologies to supplement rather than override this information.

4. Advocate with digital platforms and policymakers to encourage pro-social design and policies that recognise the contribution of civilians in addressing digital protection risks.

5. When incorporating or engaging with digital technologies in UCP practice prioritise the principles of 'Do No Harm' and 'Responsible Partnerships.'