



RESEARCH ARTICLE

# Decentred dereliction in digital international relations: PeaceTech, ethics, and the cascading of moral responsibility

Andreas T. Hirblinger<sup>1</sup> , Fabian B. Hofmann<sup>2</sup>  and Kristoffer Lidén<sup>3</sup>

<sup>1</sup>Geneva Graduate Institute, Centre on Conflict, Development and Peacebuilding, Geneva, Switzerland; <sup>2</sup>ETH Zürich, Department of Humanities, Social and Political Sciences, Zürich, Switzerland and <sup>3</sup>Peace Research Institute Oslo (PRIO), Oslo, Norway

**Corresponding author:** Andreas T. Hirblinger; Email: [andreas.hirblinger@graduateinstitute.ch](mailto:andreas.hirblinger@graduateinstitute.ch)

(Received 23 May 2024; revised 26 August 2025; accepted 1 September 2025)

## Abstract

Ethics are commonly invoked to mitigate the adverse effects of digitalization on international practices such as diplomacy, humanitarianism, or peacebuilding. However, their productive role in shaping global politics has received little attention. This article elucidates how policy and guidance documents containing 'PeaceTech' ethics discursively construct normative vectors, i.e., moral claims that frame risks, suggest responses, and attribute responsibilities. We identify five major tendencies through which this takes place, namely the internationalizing, outsourcing, delegating, localizing, and individualizing of PeaceTech-related risks. These vectors produce a cascade of responsibility that reaches from the international to the local, from the public to the private sector and civil society, and from organizations to end users. Agents placed higher in the cascade mainly deal with abstract and systemic risks, while agents placed lower are responsible for dealing with tangible and personal risks. Yet the latter often have the least resources to respond to these risks, and have to weigh up whether to accept them and maintain critical data collection and analysis functions, or to reduce these risks while potentially jeopardizing PeaceTech. We describe how this can amount to what we call 'decentred dereliction', i.e., the abandonment of goals in and through digital peacebuilding.

**Keywords:** digital technology; ethics; global politics; peacebuilding; PeaceTech; risks

Digitalization has altered most, if not all, spheres of global politics.<sup>1</sup> These include efforts to prevent conflict and build peace, where digital technologies, often referred to as 'PeaceTech', are now widely employed, such as for early warning, peace mediation, peacekeeping, and reconciliation.<sup>2</sup> The impact of digitalization is often portrayed as 'Janus-faced': digital tools are hailed for providing innovative solutions but also criticized for producing new problems.<sup>3</sup> As a result, a growing body of practice-oriented literature has begun addressing the 'ethical concerns' that come with the

<sup>1</sup>Martin Coward et al., 'On the horizon: The futures of IR', *Review of International Studies*, 50:3 (2024), pp. 415–24.

<sup>2</sup>Allard Duursma and John Karlsrud, 'Technologies of peace', in Oliver P. Richmond and Gëzim Visoka (eds), *The Oxford Handbook of Peacebuilding, Statebuilding, and Peace Formation* (2021), pp. 414–27; Kristin Anabel Eggeling and Larissa Versloot, 'Taking trust online: Digitalisation and the practice of information sharing in diplomatic negotiations', *Review of International Studies*, 49:4 (2023), pp. 637–56; Oliver P. Richmond, Gëzim Visoka, and Ioannis Tellidis, *Peace in Digital International Relations: Prospects and Limitations* (Cambridge University Press, 2023).

<sup>3</sup>Andreas Timo Hirblinger et al., 'Digital Peacebuilding: A Framework for Critical–Reflexive Engagement', *International Studies Perspectives*, 24:3 (2023), pp. 265–84.

use of PeaceTech, discussing the risks of using digital technologies for peacebuilding, as well as who should respond to them and how. This rise of what can be described as a distinct PeaceTech ethics discourse follows a more general trend to govern the effects of digitalization on international practices through ethical self-regulation.<sup>4</sup> Such dynamics are visible *inter alia* in efforts to define the ethical obligations of digital humanitarians,<sup>5</sup> or ‘principles for digital development’ for technology-enabled development programmes.<sup>6</sup>

What difference do these discussions about the ‘good’ or ‘right’ use of digital technologies make to global politics? Discussions of digital peacebuilding, in both academia and practice, often encourage wishful thinking about how PeaceTech could enable ‘bottom-up’, ‘participatory’, and ‘inclusive’ approaches that ‘empower’ and give ‘agency’ to local actors.<sup>7</sup> However, some scholars discussing the ‘transformative’ potential of digitalizing global politics have also expressed scepticism about the possibility of a ‘digital renewal’ that could overcome the pitfalls of ‘analogue’ international peacebuilding practices,<sup>8</sup> especially their tendency to both romanticize and marginalize local agency.<sup>9</sup> While the digitalization of peacebuilding has enabled approaches that are increasingly remote and decentred, thus more easily integrating actors in distant, conflict-affected, and insecure contexts, global divisions of labour, decentralized control, and a spatial distribution of power continue to shape its trajectory. This makes the digitalization of peacebuilding a good case for studying decentred global politics, which today also shape many other international practices such as diplomacy,<sup>10</sup> humanitarianism,<sup>11</sup> or development.<sup>12</sup>

Importantly, research on the decentring dynamics of digital global politics has highlighted how they may enforce a particular division of labour and distribution of material harms, spanning from Silicon Valley over Lithium mines in Bolivia to data annotators’ in Madagascar.<sup>13</sup> Can the emerging ethics of PeaceTech discourse counter these tendencies, or do the discourse merely reproduce them? What potential harms of digital peacebuilding does it identify, and what measures does it suggest for addressing them? To answer these questions, in this article we examine how the newly emerging ethics of PeaceTech contribute to the socio-technical ordering of the International, by relationally arranging a heterogeneity of semiotic and material objects employed in digital peacebuilding. In doing so, we contribute to locating morality in what has been coined the ‘missing masses’ in global governance, namely in the socio-technical systems that underpin the organization of late modern societies.<sup>14</sup> More specifically, we shed light on how the discourse on PeaceTech ethics frames technology risks, suggests responses that affect the design and use of technology,

<sup>4</sup> ‘Ethics’ originates from the Greek *ethos*, which denotes a custom or habit, and provides a ‘systematic reflection, a philosophical critique, and an evaluation thereof’: Simone Casiraghi, J. Peter Burgess, and Kristoffer Lidén, ‘Ethics and border control technologies’, in J. Peter Burgess (ed.), *Border Control and New Technologies* (Academic & Scientific Publishers, 2021), p. 81. Contrary to the norm, we use ‘ethics’ in the plural (‘are’ instead of ‘is’) given that our analysis demonstrates the plurality of ways ethics is understood and operationalized in practice.

<sup>5</sup> Stuart R. Campo, Caitlin N. Howarth, Nathaniel A. Raymond, and Daniel P. Scarnecchia, *The Signal Code: Ethical Obligations for Humanitarian Information Activities* (Cambridge: Harvard Humanitarian Initiative, 2018).

<sup>6</sup> Digital Impact Alliance, ‘Principles for Digital Development’, available at: {<https://digitalprinciples.org/principles/>}, accessed 8 September 2022.

<sup>7</sup> Ioannis Tellidis and Stefanie Kappler, ‘Information and communication technologies in peacebuilding: Implications, opportunities and challenges’, *Cooperation and Conflict*, 51:1 (2016), pp. 75–93.

<sup>8</sup> Oliver P. Richmond and Ioannis Tellidis, ‘Analogue crisis, digital renewal? Current dilemmas of peacebuilding’, *Globalizations*, 17:6 (2020), pp. 935–52.

<sup>9</sup> Roger Mac Ginty and Oliver Richmond, ‘The local turn in peace building: A critical agenda for peace’, *Third World Quarterly*, 34:5 (2013), pp. 763–83.

<sup>10</sup> Eggeling and Versloot, ‘Taking trust online’.

<sup>11</sup> Fleur Johns, *#Help: Digital Humanitarianism and the Remaking of International Order* (Oxford University Press, 2023).

<sup>12</sup> Mark Duffield, *Post-humanitarianism: Governing Precarity in the Digital World* (Polity Press, 2019).

<sup>13</sup> Kate Crawford, *Atlas of AI: power, politics, and the planetary costs of artificial intelligence* (New Haven: Yale University Press, 2021).; Clément Le Ludec, Maxime Cornet, and Antonio A. Casilli, ‘The problem with annotation: Human labour and outsourcing between France and Madagascar’, *Big Data & Society*, 10:2 (2023), p. 20539517231188723.

<sup>14</sup> Maximilian Mayer and Michele Acuto, ‘The global governance of large technical systems’, *Millennium*, 43:2 (2015), pp. 660–83.

and allocates responsibilities for implementing these responses among the heterogeneous actors participating in digital peacebuilding. We demonstrate that ethics play a productive role in the socio-technical ordering of global politics because they decentre moral agency, which unevenly attributes the responsibility for certain risks across a cascade of actors involved in digital peacebuilding. This productive role of PeaceTech ethics makes them a crucial entry point for imagining, thinking, and practising digitized international relations differently.

We make our argument based on the qualitative analysis of 44 policy- and practice-oriented documents that reflect the experiences of international organizations (IOs), non-governmental organizations (NGOs), technology conglomerates, and academic institutions working with PeaceTech, and provide practical guidance for mitigating its adverse effects. However, our analysis goes beyond engaging with the normative claims in these documents (i.e. with what the PeaceTech ethics discourse is *saying*) to critically interrogate the socio-technical ordering practices that underpin them (i.e. what the PeaceTech ethics discourse is *doing*). To this end, we draw on interviews and focus-group discussions with hate-speech monitors in Sri Lanka and conflict-early-warning monitors in South Sudan to illustrate how the underlying patterns of normative claims make it more likely that the decentred risks of digitalization will be distributed and responded to in the way we describe, and not another.

To investigate the distribution of moral responsibility, we introduce the concept of ‘normative vectors’, i.e. fact and value claims that frame risk, suggest responses, and attribute responsibilities within the socio-technical systems that constitute digital peacebuilding. We show that every claim is typically supported by a normative logic that justifies the distribution of moral responsibility in line with broadly accepted ethical perspectives. However, a bird’s-eye view on the resulting risk-response-responsibility cascade reveals what we call a ‘decentred dereliction’ that emerges in the decentralized networks of digitalized global politics: the PeaceTech ethics discourse prompts actors that are placed higher in the cascade to address the more systemic and abstract risks associated with technology use, while passing on tangible risks that may affect personal safety to actors placed lower in the cascade. This means that the final responsibility for ensuring that PeaceTech applications function and deliver is transferred from well-resourced and protected actors to more vulnerable actors, those with the least resources to respond to them. Therefore, end users, who form a critical part of the decentred arrangements of digital peacebuilding, must often decide whether to accept tangible risks to themselves or opt out of the digital peacebuilding effort. This increases the likelihood of *dereliction* of peacebuilding goals because the socio-technical networks that constitute digital peacebuilding may ultimately fail to meet their declared objectives when vulnerable end users cannot shoulder the disproportionate risks attributed to them. We describe this dereliction as *decentred* because it is not the act of a single moral agent, but unfolds in a cascade of interlinked instances of moral reasoning.

The article proceeds as follows: we first discuss how digitalization affects the decentring of global governance before introducing our approach to the socio-technical ordering of risks, responses, and responsibilities through normative vectors. After that, we present a fine-grained analysis of the risk-response-responsibility cascade. Finally, we draw conclusions for digital peacebuilding and related fields of practice that grapple with the impact of digitalization on global politics.

### Digitalization and risk in the distributed socio-technical systems of the International

The uptake of digital technologies in peacebuilding has paved the way for new approaches that are both remote and decentred. Digitalization enables remoteness through data transmission, primarily via the Internet, and this volume has grown exponentially over the past few decades.<sup>15</sup> While taking place at a globally uneven pace, this trend has impacted conflict-affected areas where dilapidated physical infrastructures are bridged via nimble mobile networks and satellite-based communication. Moreover, advancements in remote communication have enabled the decentring

<sup>15</sup>International Telecommunication Union, *Global Connectivity Report 2022* (2022).

of many international activities, including peacebuilding, catalysing the technical differentiation of functional tasks among actors with specific roles and expertise, including IOs, tech developers, and civil society actors. For instance, the design of PeaceTech mobile phone applications separates the operational headquarters of peacebuilding organizations from staff or volunteers in conflict zones via back ends and front ends, which births a spatial, functional, and often temporal decentralization of tasks. Importantly, this may also pave the way for more controlling approaches, enabling the close direction of 'ground operations' from the comfort of headquarters.<sup>16</sup>

However, the impact of digital technologies should not be overstated either. Global divisions of labour and decentralized control clearly predate the onset of digitalization and continue to shape contemporary global governance arrangements.<sup>17</sup> Notably, European imperial or colonial rule tended to rely on the integration and co-optation of local authorities and their technologies of rule to maintain 'law and order'.<sup>18</sup> Arrangements resembling such 'indirect rule' can also be found in many contemporary international efforts to strengthen peace and security. In fact, policy and guidance calling for 'localization' or 'local ownership' partly originated from colonial thought that dates back well before the Internet age.<sup>19</sup> In this thinking, local actors 'on the ground' should autonomously lead peacebuilding tasks, while staff based in the safety and comfort of headquarters or fortified field missions continue to play an auxiliary but crucial role, ranging from design to funding and evaluation of measures.<sup>20</sup> These arrangements tend to be characterized by an unequal exposure to the insecurity of conflict-affected contexts, which leaves intermediary actors disproportionately exposed to adverse effects.<sup>21</sup> For instance, African regional organizations' early warning systems rely on field-based monitors equipped with smartphones and data vouchers that send alerts from distant and dangerous locations, which are then relayed to control rooms from where data is aggregated and visualized in order to be acted upon by high-level decision-makers.<sup>22</sup>

Furthermore, mediation teams increasingly employ digital platforms to conduct digital consultations or dialogues to further the inclusiveness of peace processes in places such as Bolivia, Libya, or Yemen, simultaneously reaching hundreds of stakeholders to learn about needs, interests, and expectations that may often be politically sensitive and put them at odds with conflict parties or incumbent authoritarian regimes.<sup>23</sup> Thus, it may be best to describe digitalization as a catalyst for historically evolved forms of decentralized governance that often perpetuate violence and insecurity and are particularly convenient when security calculations and risk avoidance take centre stage.<sup>24</sup>

Significantly, digitalization shapes peacebuilding not only by offering new digital applications but also through a discourse on technology that conditions all aspects of the field, including professional conduct, organizational designs, and institutional norms. Therefore, as Hirblinger et al. put it, we should focus on how 'technologies for peacebuilding and peacebuilding with technology are coproduced', by studying how claims about technology inform how peacebuilding is conducted,

<sup>16</sup>Roger Mac Ginty, 'A material turn in International Relations: the 4x4, intervention and resistance', *Review of International Studies*, 43:5 (2017), p. 864..

<sup>17</sup>John Gerring, Daniel Ziblatt, Johan Van Gorp, and Julián Arévalo, 'An institutional theory of direct and indirect rule', *World Politics*, 63:3 (2011), pp. 377–433.

<sup>18</sup>Comfort Ero, 'Peacebuilding though statebuilding in West Africa? The cases of Sierra Leone and Liberia', in Devon Curtis and Gwinyayi Albert Dzinesa (eds), *Peacebuilding, power, and politics in Africa* (Ohio University Press, 2012), pp. 232–52.

<sup>19</sup>Andreas T. Hirblinger and Claudia Simons, 'The good, the bad, and the powerful: Representations of the "local" in peacebuilding', *Security Dialogue*, 46:5 (2015), pp. 422–39.

<sup>20</sup>Mark Duffield, 'Risk-management and the fortified aid compound: Everyday life in post-interventionary society', *Journal of Intervention and Statebuilding*, 4:4 (2010), pp. 453–74.

<sup>21</sup>Alex Veit, *Intervention as Indirect Rule: Civil War and Statebuilding in the Democratic Republic of Congo* (Campus, 2010).

<sup>22</sup>Ulf Engel, 'Knowledge production on conflict early warning at the African Union', *South African Journal of International Affairs*, 25:1 (2018), pp. 117–32.

<sup>23</sup>Daanish Masood Alavi, Martin Wählich, Colin Irwin, and Andrew Konya, 'Using Artificial Intelligence for Peacebuilding', *Journal of Peacebuilding & Development*, 17:2 (2022), pp. 239–43.

<sup>24</sup>Mark Duffield, 'The resilience of the ruins: Towards a critique of digital humanitarianism', *Resilience*, 4:3 (2016), p. 148.

and with what consequences.<sup>25</sup> The powerful effects of this co-production of the technical and the social are also visible in the ethics of PeaceTech.<sup>26</sup> We elucidate them through a discourse analysis of key policy and guidance documents that scrutinizes the normative concerns of leading actors with peacebuilding or conflict prevention mandates, including international, regional, and national governmental organizations, international and national non-governmental organizations, and think tanks.<sup>27</sup> The discursive framings of risks in these documents, and the suggestions they make to address them, matter as much as the digital applications and tools they engage with.

Importantly, the discourse on the risks of PeaceTech forms part of a broader concern with the ‘appropriate sharing of risk between local peacebuilders, intermediary INGOs, and donors across the international peacebuilding chain’,<sup>28</sup> which also extends to other fields of international governance, such as humanitarian interventions<sup>29</sup> and global health.<sup>30</sup> In such fields, the discourse on the risks associated with the use of digital technology affects the distribution of adverse effects, as well as the respective responses to it. Notably, such risk governance is always an analytical-moral hybrid, combining fact- and value-based claims that identify risks and suggest how they should be governed.<sup>31</sup> Consequently, the analysed documents not only identify the risks associated with using PeaceTech but also attribute responsibility for mitigating them, in which software developers, peacebuilding organizations, and conflict-affected communities variously have a part. We turn to this aspect next.

### The socio-technical ordering of moral responsibility in and through PeaceTech ethics

Among moral philosophers working on responsible research and innovation, the growth in ethical frameworks on responsible technology use has spurred concerns over the inflationary use of the term ‘ethics’ by policymakers.<sup>32</sup> For instance, ethicists caution about the widening gap between the use of ethics as a normative inquiry into technologies’ consequences and its instrumentalization as a political endeavour by business actors to improve their public image.<sup>33</sup> The latter, commonly referred to as ‘ethics washing’, designates the promotion of ethical industry self-regulation as an ‘easy’ alternative to regulatory solutions.<sup>34</sup> The emerging professional discourse on PeaceTech ethics exhibits similar traits. For instance, many publications on PeaceTech-related

<sup>25</sup>Hirblinger et al., ‘Digital Peacebuilding’.

<sup>26</sup>Sheila Jasanoff (ed.), *States of knowledge: the co-production of science and social order* (Routledge, 2004).

<sup>27</sup>Of the 44 documents analysed, 12 were from traditional peacebuilding organizations, such as Search for Common Ground, eight were drawn from various UN agencies, such as UN DPPA and DPO, eight from academic institutions, such as the NYU CIC, seven from ‘digital first organizations’ such as Build Up or the ICT4Peace Foundation, three from regional organizations such as ECOWAS, three from state ministries such as the German Gesellschaft für Internationale Zusammenarbeit (GIZ), and three from policy-oriented research centres such as swisspeace. See Appendix 1 for the full list of documents. The coded archive is available at [Link provided with publication].

<sup>28</sup>Jannie Lilja and Kristine Höglund, ‘The role of the external in local peacebuilding: Enabling action – managing risk’, *Global Governance: A Review of Multilateralism and International Organizations*, 24:3 (2018), p. 425.

<sup>29</sup>Dennis Dijkzeul and Kristin Bergtora Sandvik, ‘A world in turmoil: Governing risk, establishing order in humanitarian crises’, *Disasters*, 43:S2 (2019), pp. S85–108.

<sup>30</sup>Eric D. Perakslis, ‘Using digital health to enable ethical health research in conflict and other humanitarian settings’, *Conflict and Health*, 12:1 (2018), p. 23.

<sup>31</sup>Marjolein B. A. van Asselt and Ortwin Renn, ‘Risk governance’, *Journal of Risk Research*, 14:4 (2011), p. 436.

<sup>32</sup>See, for instance, Mirjam Burget, Emanuele Bardone, and Margus Pedaste, ‘Definitions and conceptual dimensions of responsible research and innovation: A literature review’, *Science and Engineering Ethics*, 23:1 (2017), pp. 1–19; Richard Owen, Phil Macnaghten, and Jack Stilgoe, ‘Responsible research and innovation: From science in society to science for society, with society’, *Science and Public Policy*, 39:6 (2012), pp. 751–60.

<sup>33</sup>Matthias Leese, Kristoffer Lidén, and Blagovesta Nikolova, ‘Putting critique to work: Ethics in EU security research’, *Security Dialogue*, 50:1 (2019), pp. 59–76. Kristoffer Lidén, ‘Ethics and the governance of digital data in humanitarian action’, *Disasters*, 50:1 (2025), p. e70018.

<sup>34</sup>Elettra Bietti, ‘“From ethics washing to ethics bashing: A view on tech ethics from within moral philosophy”’, *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery, 2020), pp. 210–9;



risks often employ ethics as a ‘buzzword’, mentioning ethical challenges in passing without engaging with them in any depth. On the other hand, many peacebuilding organizations make efforts to define and implement normative or ethical guidelines to inform their policies and practices, such as operationalizing ‘do no harm’ approaches or the guidelines subsumed under the OECD DAC<sup>35</sup> standards. These efforts impact programming and practice to some degree, making it difficult to simply dismiss them as a ‘fig-leaf’ manoeuvre.

Furthermore, the PeaceTech ethics discourse weaves together disparate ethical principles, seemingly employing them at will. This seemingly resembles ‘ethics shopping’, which occurs when there are multiple ethical principles and standards to choose from, and companies select those that match their predefined ends.<sup>36</sup> As an aspect of ethics washing, ethics shopping helps circumvent the most constraining forms of regulation and only adheres to those ethical principles that do not require changes that endanger a company’s core interests. However, the same can’t be said about policy and practice documents on PeaceTech, which often highlight the need to adhere to national legislation and stress the applicability of internationally established norms and guidance. Moreover, compared to ethics shopping in the private sector, the quagmire of ethics perspectives in digital peacebuilding produces notably different outcomes. Most of the suggested responses to risk correspond with established ethical perspectives; this seemingly ensures the ‘good use’ of PeaceTech. However, in their totality, they amount to what we call decentred dereliction, an outcome which in fact risks endangering the core interests and objectives of digital peacebuilding initiatives.

Importantly, the drawing together of different ethics perspectives in PeaceTech guidelines does more than just provide a convenient tool to avoid more profound efforts to prevent the adverse effects of technology. Based on an in-depth analysis of policy and practice documents that engage with PeaceTech and digital peacebuilding, we show that PeaceTech ethics contribute to the socio-technical ordering of international peacebuilding.

Drawing on John Law, we take an interest in such practices of ‘ordering’<sup>37</sup> to describe how the relational arranging of a heterogeneity of semiotic and material objects organizes the use of digital technologies in peacebuilding. Ordering may come ‘in the form of simple stories or accounts’ that ‘tell of what used to be, or what ought to happen’, yet they are ‘much more than narratives’ because they are ‘in some measure, performed or embodied in a concrete, non-verbal manner in the network of relations’.<sup>38</sup> While the ‘telling’ may be most accessible to the researcher, the acting out and embodying of the ordering implied in it matters just as much (ibid.). Thus, in ordering, the social and the technical are co-constitutive:<sup>39</sup> an app or database is not merely a passive extension of the discursive, as is sometimes implied in the notion of the ‘dispositif’ or ‘apparatus’,<sup>40</sup> but an integral part of it.

Therefore, we take an interest in the ordering agency of technological applications, which, among others, may affect human moral reasoning, as Michel Callon suggested: ‘[M]achines are ordering human beings around by playing with their bodies, their feelings or their *moral reflexes*’.<sup>41</sup>

Luciano Floridi, ‘Translating principles into practices of digital ethics: Five risks of being unethical’, *Philosophy & Technology*, 32:2 (2019), pp. 185–93.

<sup>35</sup> ‘DAC Standards – OECD’, available at: <https://www.oecd.org/dac/dac-instruments-and-standards.htm> accessed 6 November 2023.

<sup>36</sup> Gijs van Maanen, ‘AI ethics, ethics washing, and the need to politicize data ethics’, *Digital Society*, 1:2 (2022), p. 2.

<sup>37</sup> While Law variously referred to ‘modes’, ‘principles’, and ‘strategies’ of ordering, we content ourselves with practices, which we understand as recurring patterns of behaviour that structure the International. Emanuel Adler and Vincent Pouliot, ‘International practices’, *International Theory*, 3:01 (2011), pp. 1–36.

<sup>38</sup> John Law, *Organizing modernity* (Blackwell, 1994), p. 20.

<sup>39</sup> Jasanoff, *States of knowledge*.

<sup>40</sup> Gilles Deleuze, ‘What is a dispositif?’, in Timothy J. Armstrong (ed.), *Michel Foucault, philosopher* (New York and Toronto: Harvester Wheatsheaf, 1992), pp. 159–68.

<sup>41</sup> Michel Callon, ‘Techno-economic networks and irreversibility’, in John Law (ed.), *A sociology of monsters: Essays on power, technology, and domination* (Routledge, 1991), p. 137, emphasis added.

We argue that the effects of PeaceTech applications on the moral reasoning of those who plan, design, distribute, and employ it can be inferred from the written texts these actors produce, such as the those in the archive of policy and guidance documents we have collected. While the discursive practices (the 'saying' and 'writing' of ethics) are thus our main entry point to study the ordering of global politics in and though PeaceTech ethics, non-discursive practices (the ethical use of digital technologies) and materials (the infrastructures and devices that constitute digital technologies) matter just as much in the framing and distribution of risks and the responsibility for addressing them. Building on this perspective, we map the distribution of moral responsibility through the PeaceTech ethics discourse that orders the socio-technical networks of digital peacebuilding. Taken in turn, the moral reasoning in each document contributing to the discourse often amounts to not much more than an incomplete, inconsistent, and disjunct set of ethical considerations, equalling the kind of 'moral reflexes' that Callon observed. However, in their sum, these reflexes paradoxically order digital peacebuilding.

We are concerned with socio-technical 'ordering' rather than 'order' because the evolving discourse produces contingent rather than stable outcomes. Yet we nonetheless aim to pinpoint specific patterns of ordering that may correspond with what could be described as situated and often (partly) hidden causal mechanisms of action.<sup>42</sup> While we thus do not intend to demonstrate causality in terms of a covering law, we point to specific recurring patterns in international practice that help to explain certain outcomes in comprehensible and meaningful ways to a broad range of cognizant actors that take part in, or can observe, the socio-technical network. Such recurrence speaks of a certain 'logic' through which international peacebuilding is characterized, and this logic has powerful effects on the dynamics of peace and conflict and the humans affected by them.<sup>43</sup>

We suggest in this article that the logic with which the PeaceTech ethics discourse responds to risks involves the ordering of the moral responsibility to address them across a cascade of action domains. When building our argument, we drew inspiration from concerns about how decentralized and remote socio-technical arrangements can enable 'moral distance' or 'moral disengagement', which makes inhumane acts possible. This concept has been widely studied in the context of military technologies and the bureaucratization of warfare and mass violence. In the context of the Holocaust, Zygmunt Bauman argued that the making of moral distance 'quashes the moral significance of the act and thereby pre-empts all conflict between personal standard of moral decency and immorality of the social consequences of the act'.<sup>44</sup> Similarly, contemporary technology ethicists view digital technologies, such as drones, as central to creating moral distance, due to the loss of face-to-face contact and the invisibility of causal connections in human-machine networks with distributed agency.<sup>45</sup>

Clearly, PeaceTech differs from the use of military technologies in that it is not employed with the intention of causing harm or other actions that would be widely viewed as inhumane. Instead, the risks that uses of PeaceTech entail and the harms they may cause emerge as unintended consequences of well-intended actions. Importantly, we thus suggest that the logic through which risks become distributed works *with* – not without – morality. We explain this by showing how PeaceTech and the ethics discourse that informs its design and use create not merely remoteness and distance but decentred moral agency. We develop this aspect inspired by Albert Bandura's insight that inhumane acts can appear benign through acts of selective 'moral engagement' and 'moral disengagement', which constitute a moral agency that is notably characterized by a '*diffusion*

<sup>42</sup> Milja Kurki, 'Critical realism and causal analysis in international relations', *Millennium*, 35:2 (2007), pp. 361–78.

<sup>43</sup> William Walters, *Governmentality: Critical Encounters* (Routledge, 2012).

<sup>44</sup> Zygmunt Bauman, *Modernity and the Holocaust* (Press, 1992), p. 18.

<sup>45</sup> Mark Coeckelbergh, 'Drones, information technology, and distance: Mapping the moral epistemology of remote fighting', *Ethics and Information Technology*, 15:2 (2013), p. 93.

or *displacement* of responsibility'.<sup>46</sup> As Villegaz-Galaviz and Kirsten Martin explain in their study of AI systems, moral distance 'limits the whole comprehension of the moral context', whereas moral disengagement makes people 'convince themselves that they are causing no harm or acting wrong because ethical principles do not apply to them'.<sup>47</sup>

The case of PeaceTech ethics resembles such instances of moral distancing and disengagement in terms of its outcomes, with two important caveats. First, disengagement pertains to the reasoning about the possible adverse but unintended effects of technology, and it is enacted through a seemingly functional distribution of risks and responsibility among a cascade of actors. Tech engineers far from the application context may not only be ill-informed or ignorant regarding how peacebuilding works out 'on the ground', but may also pass on the responsibility to handle certain risks that emerge there to local moral agents. Importantly, they can do so morally because the PeaceTech ethics discourse suggests a certain division of moral labour. We can understand this process as entailing what Toni Erskine described as acts of 'attribution' that target specific 'moral agents'.<sup>48</sup> The distribution of moral responsibility along the cascade then leads to a *decentred* moral agency within the socio-technical networks that constitute digital peacebuilding, which produces moral distance. As we illustrate in this article, this decentring can ultimately cause the *dereliction* of peacebuilding objectives because it puts a disproportionate burden on those moral agents with the least resources to handle them.

Concretely, we propose to trace this distribution by mapping 'normative vectors', which we understand as patterns of fact and value claims that frame risks, suggest specific responses, and attribute responsibilities for them in line with implicit or explicit ethical perspectives. These intentional and conscious attempts at sense-making are only the most visible layer of a much broader repertoire of ordering practices, and they tend to generate simplified, romantic, and homogeneous representations of 'apparent order'.<sup>49</sup> Such representations often camouflage more conflicting practices, driven by the need for neatness and clarity that frequently haunts public policy documents. Yet, we are also sympathetic to recent calls not to fall into relational determinism by ontologically fetishizing entanglements, but instead to investigate disconnects, frictions, and resistances.<sup>50</sup> Therefore, we acknowledge that our mapping of normative vectors remains (and should remain) necessarily partial and fraught with friction – due to the contingent, situated, and somewhat superficial representation that emerges as we researchers engage with the artefacts of ordering practices. The following section provides details about how we have done this work concretely.

## Methodological note

The term 'PeaceTech' is commonly employed to refer to digital information and communication technologies (ICTs) that are specifically designed or employed to support peacebuilding efforts.<sup>51</sup> However, some of its founders have also described PeaceTech as a 'movement' of people who use technology for conflict prevention and peacebuilding.<sup>52</sup> In turn, 'peacebuilding' is notoriously difficult to define because it is commonly used as an umbrella concept to refer to a diversity of efforts

<sup>46</sup> Albert Bandura, 'Selective moral disengagement in the exercise of moral agency', *Journal of Moral Education*, 31:2 (2002), p. 116.

<sup>47</sup> Carolina Villegaz-Galaviz and Kirsten Martin, 'Moral distance, AI, and the ethics of care', *AI & SOCIETY*, 39:4 (2024), pp. 1695–706.

<sup>48</sup> Toni Erskine, 'AI and the future of IR: Disentangling flesh-and-blood, institutional, and synthetic moral agency in world politics', *Review of International Studies*, 50:3 (2024), pp. 534–59.

<sup>49</sup> Law, *Organizing Modernity*, p. 22.

<sup>50</sup> Ignasi Torrent, 'Problematising entanglement fetishism in IR: On the possibility of being without being in relation', *Review of International Studies*, 51:3 (2025), pp. 473–87.

<sup>51</sup> Pamina Firchow, Charles Martin-Shields, Atalia Omer, and Roger Mac Ginty, 'PeaceTech: The Liminal Spaces of Digital Technology in Peacebuilding', *International Studies Perspectives*, 18:1 (2017), pp. 4–42.

<sup>52</sup> Paul Heidebrecht, 'PeaceTech', *IEEE Technology and Society Magazine*, 41:3 (2022), pp. 101–2.



intended to prevent the (re)occurrence of armed conflict.<sup>53</sup> However, this vagueness does not affect the validity of our argument. Drawing on a comprehensive analysis of the policy and practice literature that constitutes the contemporary PeaceTech ethics discourse, our analysis is relevant to all those actors who self-identify as peacebuilding organizations and employ digital technologies to achieve their objectives.

Our empirical analysis focused on an archive of 44 policy and practice documents created through a systematic selection process of English-language sources published before July 2023, which we manually analysed using qualitative data analysis software. Our selection criteria were that documents needed to pertain to peacebuilding as a field of practice, have a clear practical focus, and specifically address the risks associated with using digital technologies in peacebuilding. The final sample included perspectives from different actors, namely international and regional organizations such as the United Nations and ECOWAS (the Economic Community of West African States); dedicated peacebuilding and mediation organizations such as Humanitarian Dialogue; the Berghof Foundation, Conciliation Resources, and Search for Common Ground; research centres such as swisspeace, the Toda Peace Institute or the United States Institute of Peace; (Peace)tech organizations such as Build Up; and private sector providers such as Remesh. The various documents cover the ethical concerns raised by a broad array of technologies (social media, Geographic Information Systems, online dialogues, AI, big data, etc.) in different areas of application (ceasefire monitoring, conflict early warning, peace mediation, peacekeeping, etc.).

We acknowledge that, due to our focus on English-language sources, these perspectives primarily reflect the concerns of Western-based actors rather than those based in the Majority World. However, this geographic distribution also echoes the division of labour in the 'tiered global data economy', which expresses itself, for instance, through the outsourcing of social media content moderation and AI model training by Western technology companies that, at the same time, maintain the lead in technology development and in discourses about their regulation.<sup>54</sup> A similar tendency is visible in the PeaceTech field. While local, bottom-up innovation has been part of the PeaceTech movement from the outset, the bulk of policy and guidance documents we reviewed were not produced in the Majority World but in countries where IOs and tech companies are headquartered.<sup>55</sup> This is also where the audience is based to which we address our critical analysis.

Following a 'grounded theory' approach,<sup>56</sup> we started by closely reading the policy and practice documents to code all quotations that mentioned PeaceTech-related risks, called for a specific response, and attributed responsibility for this action. Importantly, sometimes documents do not state the responsibility explicitly but imply it in the proposed response; for example, when calls are made for increased local ownership of PeaceTech interventions that morally engage local project partners or participants. These instances were coded with the implied responsibility and, at times, multiple responses.<sup>57</sup>

From this initial coding emerged our realization that the PeaceTech ethics discourse is informed by normative logics that largely correspond with three established ethics perspectives. First, 'duty-based' or deontological ethics perspectives codify PeaceTech use as ethical when it is in accord with a given set of policies or standards, such as 'do no harm' or 'local ownership', and as unethical when

<sup>53</sup>Michael Barnett, Hunjoon Kim, Madalene O'Donnell, and Laura Sitea, 'Peacebuilding: What is in a name?', *Global Governance*, 13:1 (2007), pp. 35–58; Hirblinger et al., 'Digital Peacebuilding'.

<sup>54</sup>Kai-Hsin Hung, 'Artificial intelligence as planetary assemblages of coloniality: The new power architecture driving a tiered global data economy', *Big Data & Society*, 11:4 (2024), p. 3.

<sup>55</sup>Sanjana Hattotuwa, *Untying the Gordian Knot: ICT for Conflict Transformation and Peacebuilding* (ICT4Peace Foundation, 2004).

<sup>56</sup>Janice M. Morse et al., *Developing Grounded Theory: The Second Generation Revisited* (Routledge, 2021), p. 157.

<sup>57</sup>To establish the inter-coder reliability of these assignments, the initial coding conducted by author 2 was reviewed by author 1, discussed by author 1 and 2, and then revised accordingly. As for the normative vectors, an initial sample of codes was reviewed by author 3, discussed by all authors and the coding was built on the jointly established working definitions.

it deviates from such a 'law conception of ethics'.<sup>58</sup> Second, 'consequence-based' or teleological ethics perspectives try to anticipate the normative concerns raised by digital peacebuilding applications *ex ante*<sup>59</sup> through 'risk-based' approaches or 'cost-benefit analyses' that attempt to examine these actions' contribution to the overall good of society. Third, virtue-based ethics perspectives frame digital risks as not based on rules (duty-based perspectives) or outcomes (consequence-based perspectives), but rather on the character dispositions of individual actors and actants, calling for the development of specific positive character dispositions<sup>60</sup> or skills building among PeaceTech developers and practitioners as a response to the risks associated with digital technology use.

Across the 44 documents analysed, we coded 1,334 instances of these three ethics perspectives, 1,255 responsibility attributions, and 1,274 suggested responses. These 'in vivo codes' were then clustered into increasingly abstract code groups based on shared attributes. This process resulted in 15 distinct normative vectors that distribute moral responsibility among different categories of actors located at various places and levels of the decentred digital peacebuilding network. Based on our reading of existing research on risk-sharing and adaptation in multi-scalar peacebuilding,<sup>61</sup> we are particularly interested in understanding the distribution of moral responsibility across scales (international, national, local), governmental entities (IOs, national, and sub-national governments), and non-governmental actors (civil society, private sector).

The targets of the normative vectors were identified by clustering all actors made responsible for addressing PeaceTech-related risks into five overarching domains of action, displayed in Table 1 namely the 'international domain'; the 'third-party domain', composed of the private sector and academia; the 'field domain', composed of staff working in conflict-affected settings; the 'local domain', consisting of civil society groups and community-based organizations; and the 'user domain', composed of individual end users. We suggest understanding these domains as partly hierarchical and partly nested, mixing scalar, institutional, and professional attributes. For instance, an individual user can assume moral responsibility within their user domain, which can be part of either the local domain or the field domain. This makes our cascade less neat but aligns with our understanding of socio-technical ordering as a messy process without introducing an unduly neat typological separation (see Figure 1).

To shed further light on how the PeaceTech ethics discourse affects peacebuilders in the local domain, we draw on insights from interviews and focus groups with staff and volunteers of local civil society organizations (CSOs) in Sri Lanka and South Sudan, conducted from 2021 to 2024. These research participants contributed to a four-year research project on digital peacebuilding, which compared how different degrees of digitalization and variations in the political context shape peacebuilding dynamics and outcomes. Their responses provide suitable insights because during the time of research, both cases were characterized by comparatively high levels of political repression affecting the digital realm, while civil society had a comparatively low capacity to respond to digital risks.<sup>62</sup> We conducted 11 interviews with Sri Lankan CSO staff that discussed their experiences collaborating with IOs to monitor, analyse, and respond to harmful speech on social media with the aim of preventing offline violence and predicting future conflict outbreaks. Moreover, we conducted 16 interviews and three focus group discussions with staff and volunteers working on

<sup>58</sup> Anaïs Rességuier and Rowena Rodrigues, 'AI ethics should not remain toothless! A call to bring back the teeth of ethics', *Big Data & Society*, 7:2 (2020), p. 3.

<sup>59</sup> See Carol Levine, 'Analyzing Pandora's box: The history of bioethics', in Lisa A. Eckenwiler and Felicia Cohn (eds), *The ethics of bioethics: mapping the moral landscape* (Baltimore: Johns Hopkins University Press, 2007), pp. 3–23.

<sup>60</sup> Rosalind Hursthouse, *On Virtue Ethics* (Oxford University Press, 1999).

<sup>61</sup> Lilja and Höglund, 'The role of the external in local peacebuilding'; Elisa Randazzo and Ignasi Torrent, 'Reframing agency in complexity-sensitive peacebuilding', *Security Dialogue*, 52:1 (2021), pp. 3–20.

<sup>62</sup> This research design was not chosen in order to make general claims of causality between the PeaceTech ethics discourse and local digital peacebuilding practices, but to demonstrate that our argument and analysis are relevant for cases with similar characteristics. For more details on these contexts, see Andreas T. Hirblinger, *Digital Peacebuilding? The Socio-Technicality of Transforming Armed Conflict* (Oxford University Press, forthcoming).

**Table 1.** The Five Target Domains and Corresponding Actors.

Domains	Actors
International Domain	UN agencies (e.g., UNDP, UN DPPA, DPO), international donors, regional organizations (e.g., EU, ECOWAS), state ministries (e.g., GIZ, DFID), INGOs (e.g., Mercy Corps, Search for Common Ground, Conciliation Resources, International Alert)
Third-Party Domain	Technology companies (e.g., X, Meta, Remesh), technology designers, academic institutions (e.g., NYU CIC, EUI), practice- and policy-oriented research centres (e.g., ICT4Peace Foundation, Toda Peace Institute, USIP)
Field Domain	UN country offices (e.g., UNDP country offices), UN peacekeeping operations (e.g., UNSMIL), embassies, INGO country offices (e.g., Search for Common Ground country offices)
Local Domain	Local CSOs (e.g., local peacebuilding organizations in the ECOWAS region, women's groups, youth councils, journalists, fact-checking services, human rights groups)
User Domain	UN in-country staff (e.g., mediators, UNDP personnel), UN peacekeepers on mission, local participants in digital peacebuilding projects (e.g., community-level monitors for conflict early warning, participants in digital dialogues and consultations, online hate-speech monitors)

mobile phone-based conflict early-warning systems in South Sudan, in which we asked about the context of these efforts and related challenges. The illustrative examples cited in this article highlight the attribution of moral responsibility to the field and local domains, and the unequal burden this puts on the local participants of digital peacebuilding projects.

In the following, we will substantiate our argument on the PeaceTech ethics discourse's cascading of moral responsibility on the basis of our empirical material.

### The risk-response-responsibility cascade

*How does the PeaceTech ethics discourse frame risks, suggest responses, and attribute responsibility?*

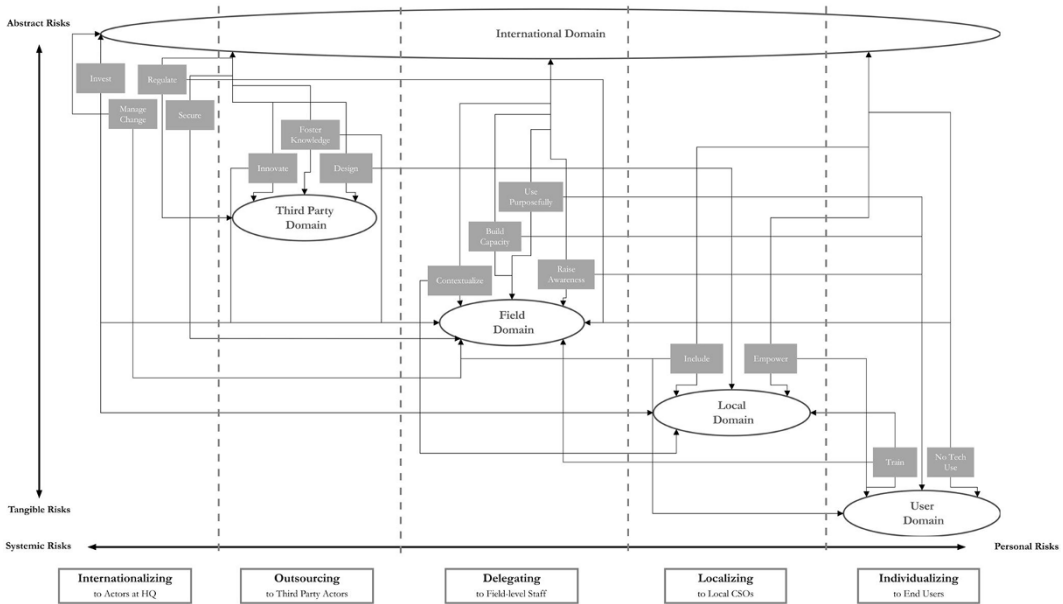
To answer this question, we trace the normative vectors underpinning the discourse that distribute moral responsibility through selective moral (dis-)engagement. For instance, a bird's-eye view of the 15 normative vectors we identified reveals how specific responses, such as empowerment, inclusion, training, or no technology use, commonly target a particular domain of activity, such as the local or end-user domain. The resulting pattern of moral (dis-)engagement is presented in [Table 2](#), where the table columns represent the five main target domains of the normative vectors, and the table rows indicate the concrete responses suggested by the PeaceTech ethics discourse for each domain. For instance, the response to 'regulate' the use of PeaceTech (third row from the top) is targeted at actors within the international domain, whose responsibility it becomes to coordinate and standardize their normative frameworks and share best practices. For each row, the target domains most frequently associated with a particular response are shaded in grey to elucidate the distinctive patterning of responsibilities within the discourse. The shaded boxes for each row add up to at least 75% of all co-occurrences between the particular response and various domains, indicating the emerging pattern of moral (dis-)engagement that the normative vectors give rise to.

By grouping those normative vectors that are aimed at the same target domain together, we identified five main tendencies that lead to the cascading of risks and responses through the observed patterns of moral (dis-)engagement, namely the *internationalizing*, *outsourcing*, *delegating*, *localizing*, and *individualizing* of moral responsibilities (see row names in bold in [Table 2](#)). Overall, these five tendencies amount to a cascading of moral responsibility from the international domain, i.e. internationalizing responsibility, to the user domain, i.e. individualizing responsibility. [Figure 1](#) illustrates this cascade based on a reduced network drawing representing the 15 normative vectors as well as the five main tendencies and associated target domains.<sup>63</sup>

<sup>63</sup>For each response type, only the most frequent co-occurrences are represented as an edge (arrow) in the network, while making sure that the displayed edges account for at least 75% of all co-occurrences between that particular response types and various moral agents.

**Table 2.** The 15 Normative Vectors and Their Five Target Domains.

	International Domain Gr = 487	Third-Party Domain Gr = 224	Field Domain Gr = 452	Local Domain Gr = 256	User Domain Gr = 216
Internationalizing	41%	11%	29%	11%	7%
Invest	49%	8%	15%	22%	6%
Gr = 82					
Manage change	38%	11%	39%	8%	4%
Gr = 149					
Regulate	47%	18%	16%	8%	10%
Gr = 110					
Secure	38%	8%	38%	9%	7%
Gr = 121					
<b>Outsourcing</b>	<b>31%</b>	<b>25%</b>	<b>19%</b>	<b>16%</b>	<b>10%</b>
Design	29%	28%	12%	17%	13%
Gr = 135					
Foster knowledge	30%	27%	22%	15%	6%
Gr = 153					
Innovate	30%	22%	27%	12%	10%
Gr = 92					
<b>Delegating</b>	<b>25%</b>	<b>11%</b>	<b>39%</b>	<b>12%</b>	<b>14%</b>
Build capacity	19%	11%	42%	12%	16%
Gr = 116					
Contextualize	28%	11%	34%	14%	12%
Gr = 118					
Raise awareness	19%	6%	50%	11%	14%
Gr = 78					
Use purposefully	30%	12%	36%	8%	15%
Gr = 114					
<b>Localizing</b>	<b>26%</b>	<b>9%</b>	<b>19%</b>	<b>26%</b>	<b>21%</b>
Empower	29%		12%	33%	17%
Gr = 121					
Include	22%	6%	24%	22%	25%
Gr = 159					
<b>Individualizing</b>	<b>17%</b>	<b>6%</b>	<b>41%</b>	<b>16%</b>	<b>20%</b>
No technology use	19%	2%	41%	10%	29%
Gr = 45					
Train	15%	8%	40%	18%	19%
Gr = 104					



**Figure 1.** The Risk-Response-Responsibility Cascade.

The cascade consists of a reduced network drawing of the 15 normative vectors (shaded boxes) and the respective target domains (ellipses). The five tendencies are represented by the dotted lines and spelled out in the boxes at the bottom of the figure. The cascade dimensions are defined by the continuum of abstract-tangible risks (y-axis) and systemic-personal risks (x-axis).

Importantly, the higher an actor is placed in this distribution, the more systemic and abstract the risks are, meaning they may affect institutional, political, or economic objectives, for instance. The lower an actor is placed, the more personal and tangible the risks within this domain become, which may affect the user's safety and well-being. The ethical perspectives that frame PeaceTech-related risks play a critical role in this cascade: consequence- and duty-based ethics perspectives underpin the PeaceTech ethics discourse's tendency to internationalize, outsource, and delegate responsibilities. On the other hand, virtue-based risk framings morally engage the lower levels of the cascade, combined with a duty-based reasoning of 'local empowerment' that drives the localizing tendency of the discourse, and consequence-based thinking that strengthens the individualization of responsibility.

In the following sections, we will reconstruct this cascading of risks, responses, and responsibilities by narrating from the point of view of the respective target domain how the PeaceTech ethics discourse morally calls on them to respond to specific risks. In this narration, we will directly refer to the document archive that constitutes the ethics of PeaceTech discourse, published in the open-source repository as part of the Supplementary Materials, referencing documents and quotations in the following pattern: D1:Q1 = Document 1, Quotation 1. Findings regarding the individualization of responsibility are further supported by first-hand accounts from the interviews and focus groups conducted in Sri Lanka and South Sudan.

### *Internationalizing responsibility*

Most of the documents in the archive are written by actors in the international domain, such as staff headquartered in New York, London, or Geneva. They provide strategic guidance and recommendations for senior management of international peacebuilding organizations on mitigating risks associated with designing, using, and maintaining ICTs for peacebuilding. This is not entirely surprising, as digitalization is widely viewed as an international phenomenon that requires an



international response, and many organizations involved in drafting these documents aspire to participate in it. However, while many of these digital risks span international and national levels, it is far from self-evident why IOs, INGOs, and peacebuilding organizations are best positioned to respond to them. Thus, it is worthwhile noting that the PeaceTech ethics discourse exhibits a tendency to *internationalize the risks of digital peacebuilding and the responsibilities to act upon them* through normative vectors that target the international community, for instance, by providing ‘access to data, generating research, building capacities, and connecting actors in the data for peacebuilding and prevention field’ (D37:Q41).

The normative vectors that contribute to the ethics discourse’s tendency to internationalize responsibilities frame the adverse effects of digital peacebuilding as primarily structural in nature. For instance, such policy and practice documents highlight the ‘inherent vulnerabilities’ (D43:Q111) of digital technologies, their potential to ‘produce biased results’ (D43:Q93), or the ‘risks from online security’ (D6:Q23) associated with their use. Adding to these risks, most publications also scrutinize the systemic adverse effects that arise from the ‘design, algorithms, and moderation policies’ (D39:Q35) of big tech companies, such as X, Facebook, or Google, and the peacebuilding sectors’ ‘dependence on external actors’ (D23:Q52) when using ‘off-the-shelf tools and platforms’ (D23:Q37). In response to these systemic risk framings, actors within the international domain are prompted through normative vectors to take strategic and long-term action, mainly focused on four areas of intervention. First, the moral engagement of senior management works through the quest to manage change, both in terms of potential threats and future technological developments, through anticipation, ‘threat modeling’ (D25:Q41), and appropriate staffing and budgeting that allows for ‘flexible approaches rather than uniform or static alternatives’ (D26:Q36). Second, the ethics discourse recommends that international actors regulate PeaceTech developments and use through normative frameworks or a ‘Code of Honor for tech company engagement in peace and conflict’ (D39:Q59). Third, digital security measures, such as information security guidance, privacy and anonymization standards, and data protection plans, are discursively framed as crucial for enhancing the ‘accountability and security’ of digital peacebuilding interventions (D13:Q175). Finally, international donor agencies are morally engaged through calls for increased investment in PeaceTech interventions to encourage innovation to ‘match the adaptability of malign actors’ (D24:Q30).

The internationalization of responsibilities is mainly driven by consequence- and duty-based logics underpinning the discourse. On the one hand, the systemic and abstract risks of digital peacebuilding are framed in consequentialist terms as stemming from a lack of flexibility, digital readiness, or insufficient funding, resulting in a situation where ‘organizational processes (...) are at odds with the pace of technological change’ (D12:Q13). On the other hand, a duty-based logic underpins the calls to uphold internationally recognized ‘do no harm’ (D8:Q23) and ‘privacy’ (D17:Q33) principles when regulating the use of digital technologies for peacebuilding. In sum, actors within the international domain are morally compelled by normative vectors to respond to the structural, global, and immaterial risks of PeaceTech through strategic, long-term action, guided by both duty-based and consequence-based logics. In the following subsection, we will move further along the cascade and highlight the distribution of risks, responses, and responsibilities within the targeted third-party domain.

### **Outsourcing responsibility**

Another group of normative vectors frames some risks as cross-cutting and, therefore, as of shared concern to different actor groups. For example, one publication notes that ‘the private sector is light years ahead in leveraging machine learning, AI, and data analytics tools for [its] businesses’, and therefore suggests that the peacebuilding practice community has ‘a lot to learn from the private sector’.<sup>64</sup> At the same time, the private companies providing these tools risk incurring reputational

<sup>64</sup>NYU CIC, *Data for Peace and Security: Report of the Practitioners Workshop on Harvesting Best Practices and Building a Community of Practice* (NYU Center on International Cooperation, 2019), p. 4.

damage if they do not collaborate with PeaceTech initiatives in fighting polarization and harmful speech on their platforms. Similarly, the lack of knowledge on ‘what types of programs work and in what contexts’ (D14:Q13) is a recurring concern across the archive. Often, it is accompanied by the call to engage in partnerships ‘with researchers and academics to add to the literature of whether technology increases systematic bias or errors’ (D8:Q49). In short, the design, user policies, and community standards of digital platforms, as well as a lack of knowledge about the ‘unintended effects’ of digital peacebuilding (D27:Q19), are framed in the PeaceTech ethics discourse as cutting across different domains of activity.

Against this background, third parties are morally tasked with finding solutions to these cross-cutting issues, a discursive tendency we refer to as the *outsourcing of risks, responses, and responsibilities* through normative vectors targeting the third-party domain. On the one hand, technology companies are called upon to improve the design of their platforms and applications and help peacebuilding organizations innovate and use ‘new methods and tools as AI and ML for processing, analyzing, or predictive modeling’ (D37:Q71). This could be achieved, for example, through ‘public and private PeaceTech funds to accelerate technological applications for peace’ (D2:Q7). Innovation could spring from ‘AI/tech hubs and open collaboration platforms that gather data scientists and ML experts’ (D37:Q41) and could help build a ‘culture of innovation’ (D44:Q23) within the (digital) peacebuilding sector. Moving from the private sector to academia, the ethics discourse expresses the ‘need for increased research and assessment’ (D14:Q13) of PeaceTech initiatives and their impact, thereby morally engaging research institutions, think tanks, and consultancies. Such calls to foster knowledge address the need for a ‘greater evidence base’ (D24:Q11) in digital peacebuilding, which could help mitigate its harmful effects.

This outsourcing of responsibility is informed by different ethical perspectives. Consequence-based logics frame the adverse effects of technology as rooted in a lack of knowledge about its potential consequences and attribute the responsibilities for addressing them to actors within academia. Moreover, outsourcing to third-party actors is also partially driven by duty-based thinking, which calls on tech companies to make the design of their tools, applications, and platforms more ‘human-centered’ (D37:Q46), ‘openly accessible’ (D23:Q28), and ‘context-relevant’ (D31:Q11). The duty-based ethical perspectives that discursively push towards this outsourcing of responsibility are also implicated in the localizing and individualizing tendencies discussed further below. Finally, when outsourcing responsibilities from international peacebuilding actors to private companies, the policy and practice documents also often employ a virtue-based language that specifically engages technology designers as moral agents, given that ‘the values of technology developers (...) influence how technologies function’ (D23:Q20).

In sum, the normative vectors underpinning the archive are prone to associating risks stemming from the design and user policies of digital technologies, as well as a lack of knowledge about their unintended consequences, with third-party actors, such as academics and think tanks, technology companies, and start-ups. We describe the moral engagement of these actors from the third-party domain as an outsourcing of risks and responsibilities, which entails collaborations with organizations to foster knowledge, a culture of innovation, and improve the design of ICTs for peace. However, the more tangible risks associated with introducing these digital technologies into a fragile or volatile political context, along with the necessary mitigation measures that need to be implemented, are cascaded further down to the field domain, as we will demonstrate in the next section.

### ***Delegating responsibility***

The field domain contains actors who are often portrayed as ‘field-based’ (D23:Q2), ‘on the ground’ (D43:Q25), or ‘in mission’ (D37:Q54), and who are tasked with implementing the strategic priorities defined in the international domain and responding to the arising practical challenges. The PeaceTech ethics discourse describes these actors as ‘peacekeepers’ (D12:Q52), ceasefire ‘monitors’ (D19:Q41), and in-country ‘mediators’ (D43:Q101), who need to ‘understand the interaction

of digital technologies in the conflict environment and reduce the risk of inadvertently causing harm' (D43:Q101). The negative effects of digital peacebuilding are then framed as primarily stemming from PeaceTech interventions that can 'have the unintended consequence of perpetuating or creating new forms of exclusion' (D43:Q79) through 'technology use, due to location, literacy, socio-economic constraints, etc.' (D4:Q60). In contrast to the more abstract risk perceptions higher up the risk-response-responsibility cascade, these adverse effects of digital peacebuilding are framed as more concrete, testifying to a concern that PeaceTech should be 'contextually appropriate' (D8:Q21) and that it should be 'deployed, monitored, and used, in an ethical manner' (D37:Q20).

In light of such considerations, the normative vectors targeting this domain suggest several responses that amount to the *delegating of risks, responses, and responsibilities* that morally engages actors within the field domain. For instance, having a 'body of staff that is technology-aware and data literate' (D12:Q63) is portrayed as a crucial success factor across the archive. This could be achieved by raising awareness about digital peacebuilding harms and building the capacity of actors within the field domain to 'choose the technological tools which best support their priorities while being aware of any limitations imposed by threats to the process' (D25:Q25). For instance, the authors of a report on the use of digital technologies in peace mediation argue that support actors should 'build capacity within mediation teams to create awareness of the potential value (and limitations) of social media analysis', which would put teams in a 'position to decide whether to conduct analysis in-house or to collaborate with external partners'.<sup>65</sup>

Furthermore, these actors are morally engaged through calls to implement a 'do no harm approach and conflict sensitivity' (D37:Q3) in PeaceTech interventions. On the one hand, such discursive framings make actors 'on the ground' responsible for contextualizing digital peacebuilding activities based on 'an understanding of (...) the different levels of internet access and technical capacities of the actors using social media' (D29:Q80), and sensitivity to 'gender, ethnicity, religion, political affiliation, sexual conduct and sexual orientation' (D13:Q170). On the other hand, the ethics discourse associates the field domain with the *purposeful* use of digital technologies in fragile or volatile sociopolitical settings in accordance with peacebuilding norms and guiding considerations, such as 'do no harm' (D43:Q126), 'due diligence' (D32:Q7), and 'duty of care' (D42:Q112).

Based on these response strategies, we can uncover the virtue-based, consequence-based, and duty-based logics that guide these vectors to target actors 'on the ground'. Awareness-raising and capacity-building measures are framed using virtuous terms, focusing more on the moral agent and their positive character dispositions than on the response. For instance, most documents agree that actors within the field domain 'must be first aware of the risks that they are exposed to in their work' (D27:Q95), which entails a 'need to focus on building capacity' (D36:Q16). Moreover, a consequence-based ethics perspective concerned with the 'unintended consequences of tech' (D4:Q75) informs the moral engagement of peacekeepers, conflict monitors, and digital peacebuilders to practically implement 'context-' (D36:Q52) or 'conflict-sensitivity' (D39:Q69) principles. Finally, the purposeful use of digital technologies in peacebuilding is underpinned by a duty-based logic that promotes the 'responsible use of digital technologies' (D12:Q49), in line with principles and frameworks originating in the international domain.

Admittedly, this sharing of responsibilities between the international and field domains is nothing new, nor is it exclusive to digital peacebuilding. However, the PeaceTech ethics discourse illustrates how the distribution of moral responsibility also entails a vertical shift in risk awareness, with actors in the international domain mainly focused on strategic, long-term planning in response to more structural and global risks. In contrast, the more tactical responses to the negative effects associated with peacebuilding practice are left to the field level. While, of course, many documents in the archive also mention how international actors need to be aware of PeaceTech-related

<sup>65</sup>David Lanz, Ahmed Eleiba, Enrique Formica, and Camino Kavanagh, *Social Media in Peace Mediation: A Practical Framework* (New York: UNDP and swisspeace, 2021), p. 8.

risks, this is more often implied rather than stated explicitly, whereas actors 'on the ground' are more directly targeted by normative vectors calling for awareness and sensitization. For instance, the discourse primarily portrays it as the mediators' 'responsibility to be aware of the risks of using a particular technology' (D25:Q17) or for digital analysts to 'be aware of potential issues of selection bias, trustworthiness of information, and security and privacy of users' (D8:Q38). Such moral engagement of actors within the field domain goes beyond a mere division of labour within international peacebuilding. Instead, it highlights the discursive cascading down of more tangible risks, which also extends to local CSOs, such as 'local journalists and bloggers' (D29:Q52), and eventually to 'the user' (D13:Q180) of PeaceTech. The following sections will further unpack this.

### *Localizing responsibility*

Regarding the design and implementation of digital peacebuilding activities, a core concern expressed in the discourse extends to the risk of disempowering conflict-affected populations. Examples include 'top-down' uses (D10:Q3) of digital technologies, such as through 'one-way' or 'mass communication' (D27:Q62), remote-sensing, and analytical approaches that extract data without actively involving populations and making the data available to them (D23:Q8); opaque algorithmic models that generate inexplicable results; or superficial interventions that do not provide opportunities for meaningful engagement. There are also concerns that digital approaches could curtail the rights of conflict-affected populations, including by affecting their privacy or freedom of expression (D43:Q83). Disempowerment could result from new exclusions due to unequal digitalization, including through limited digital access and literacy of parts of the population, limited financial and technical resources to procure and maintain technologies (D27:Q14), and the bypassing of certain conflict stakeholders or parties (D27:Q105), which further stratifies who can participate in – and benefit from – digital peacebuilding (D39:Q48). The ethics discourse also often references the disproportionate power of large technology companies, especially social media platforms, which may steer approaches to digital peacebuilding and offer solutions that do not meet a population's needs (D23:Q52).

In formulating a response, the PeaceTech discourse highlights the role of actors in the local domain, including civil society and community-based organizations. These actors are called upon to make PeaceTech more 'locally relevant' (D39:Q98), foster 'local ownership' (D15:Q14), and ensure 'that technology development is driven by local problems rather than external solutions' (D10:Q3). All this amounts to a discursive *localization of risks, responses, and responsibilities* through the moral engagement of local actors via normative vectors that target CSOs and other local organizations. Within the ethics discourse, localization is primarily informed by duty- and virtue-based logics that invoke local empowerment as a normative principle, often referencing a broader discourse in international peacebuilding policy and practice associated with the 'local turn'.<sup>66</sup> However, given the widespread acceptance of this principle among the policy and practice communities, the overarching moral arguments for localization are often not made explicit. Instead, the archive frames undermining the principle of local empowerment in and of itself as a risk (D39:Q29; D23:Q2), or states that promoting local agency is a moral imperative (D36:Q24). However, at times, the ethics discourse also frames localization as a means to prevent 'unintended tech harms' (D39:Q29) or address risks compounded by disempowerment, such as the fact that populations may have limited trust in digital initiatives (D19:Q27; D32:Q32).

A related motif can be found in normative vectors that advocate for digital *inclusion*, which, while not necessarily invoking the notion of the local, encourage the active participation of ordinary citizens in digital peacebuilding. Calls for inclusion are driven by an ethical perspective that is partly duty-based and partly consequentialist. On the one hand, it is rooted in a discourse regarding the imperative of equal participation (particularly of women, but to some extent also of other

<sup>66</sup>Mac Ginty and Richmond, 'The local turn in peace building.'

genders and sexual minorities). On the other hand, it builds on a functionalist argument that broad-based and diverse peacebuilding efforts will be more legitimate, empowering (D27:Q64; D32:Q12), and sustainable, or have other strategic value, such as producing relevant evidence to support peace processes (D28:Q21). In practice, normative vectors that underpin calls for inclusion and local participation often overlap, engaging a similar set of actors – namely, CSOs located within the local domain. The ethics discourse morally engages local actors, often described as from groups that are ‘underrepresented’ or ‘marginalized’, in an effort to reduce structural inequalities (D23:Q65); for instance, by stating that they must have ‘voice’ (D23:Q98; D23:Q2), or ‘claim the digital space as their own’,<sup>67</sup> resulting in a localization of risk mitigation through increased inclusion and the empowerment of locally owned and managed PeaceTech initiatives. This necessarily means that other actors further up the risk-response-responsibility cascade, such as those within the international or field domain, will partially relinquish or share their moral responsibility in mitigating further adverse effects from digital peacebuilding.

As described in relation to the third-party domain above, the cascade distributes various responsibilities among multiple moral agents in a manner that fosters shared moral engagement. Outsourcing risks and responsibilities also entails making digital technologies fit for purpose by enhancing private sector expertise with local knowledge, ensuring that ‘data-driven approaches are driven by local needs and decisions’ (D37:Q57). While some documents across the archive advocate for experimentation with and the employment of new technologies in this regard, others suggest that localization can also be achieved ‘on the cheap’. Several contributions suggest coping with limited local capacities by employing simpler off-the-shelf tools, leaving ‘locals’ with ‘cheaper and less elaborate digital tools’ (D23:Q88). Such an approach to outsourcing and localizing risks and responsibilities means that actors who are already likely to be less privileged, given their relative lack of ‘digital capital’,<sup>68</sup> will have less advanced technologies with which to respond to PeaceTech’s disempowering effects. Moving further along the risk-response-responsibility cascade, the final section will explore the adverse effects distributed to the user domain.

### *Individualizing responsibility*

Across the PeaceTech ethics discourse, normative vectors calling for localization and digital inclusion often target the ‘beneficiaries’ or ‘end users’ of technology. These actors are recognized as the most vulnerable to exclusion and marginalization through digital technology, as well as the most exposed to tracking, surveillance, and physical security risks. For instance, a UN report on remote ceasefire monitoring found that ‘the use of mobile technology would place the civil society monitors in greater personal danger, in part due to issues around limited data security and digital literacy’ (D19:Q44). Among the international and third-party domains, these personal and tangible risks, which affect the physical security and personal safety of end users, are only partially addressed, as their strategic responses focus mainly on systemic and abstract risks. Instead, the risks of censorship, surveillance, and offline harms are cascaded down to the field, local, and user domains, where, eventually, individuals are left with the responsibility for taking concrete action.

We describe this attribution of moral responsibility by the PeaceTech ethics discourse as a tendency to *individualize risks, responses, and responsibilities* through normative vectors that target the end users of digital peacebuilding tools. This tendency is primarily driven by virtue- and consequence-based logics, which combine the belief that costs can be minimized with the implementation of risk-reduction measures undertaken by a virtuous end user. Often suggested in this regard are individual training measures aimed at ultimately increasing end users’ willingness and capacity to respond to risks. Some documents in the archive promote the training of ‘newcomers to the online space’, thereby morally engaging end users in the normative quest to ‘promote digital

<sup>67</sup> Alice Coulibaly and Jo Dodd, *Pioneering Peace: Digital Inclusion and Adaptation in Response to COVID-19* (PeaceDirect, 2021), p. 41.

<sup>68</sup> Massimo Ragnedda, *The Third Digital Divide: A Weberian Approach to Digital Inequalities* (Taylor & Francis, 2017).



inclusion and participation' in PeaceTech activities (D27:Q82). While such framings speak more to the risk of disempowerment and exclusion, other contributions address the concerns raised by tracking and surveillance more directly. In response, they recommend the following: 'train users to disable Wi-Fi, cellular data signals and GPS when they are gathering or sending data' (D13:Q56). Besides conflict-affected communities engaged through PeaceTech interventions, most contributions locate individual skill-building measures among staff in field missions, local organizations, or with volunteers in CSOs that engage with PeaceTech projects. Cognizant of the hurdles and risks that a lack of digital literacy poses, responses that call for more training advance individual-level skill-building on 'cyber-security measures' (D3:Q66).

This tendency to individualize moral responsibility is well encapsulated in the growing interest in 'cyber hygiene'. Such personal-level security measures are intended to protect users from surveillance, information security threats, and privacy risks. They have experienced a surge in the context of the COVID-19 pandemic and increased teleworking. Just like sanitary hygiene, cyber hygiene is framed in the PeaceTech discourse as an individual responsibility, which seeks to control risk through disciplinary measures that regulate the conduct of individual subjects. It is rooted in the understanding that 'many risks can be mitigated with basic, accessible safety practices' (D40:Q10). For instance, the UN Mediation Support Unit's online course on Digital Risk Management advises end users on the use of VPNs to establish secure Internet connections, the dangers of external storage devices, and issues that can arise from state and private data protection policies (D42:Q27; D42:Q54). The ethical perspective that encourages the individualization of risks and responsibilities is thus at least partly consequence-based, making the point that costs could be most efficiently and effectively reduced by morally engaging end users.

The reasoning for attributing the responsibility to handle such risks to individual users seems to be partly grounded in the insight that controlling for such risks is (nearly) impossible in decentred arrangements. As one report puts it succinctly, 'It will never be possible to be 100% secure online. The most effective defence against malware and other malicious activity is often your own behaviour'. (D42:Q84). Many other contributions also provide tips regarding the safe storage, transfer, and management of data, while emphasizing that, in a team environment, digital security 'is only as good as the weakest link' (D34:Q12). Rather than engaging better-resourced agents in other domains further up the risk-response-responsibility cascade, some contributions even call for individual users to shoulder this moral responsibility instead. This trend is captured in the terminology of 'resilience' across the archive, which designates both an individual and collective capacity to withstand threats in cyberspace (D27:Q114; D14:Q74; D23:Q124). As one contribution put it, when discussing risks such as misinformation and hate speech, responses that emphasize knowledge-sharing and skills building and that ultimately aim to provide 'tools for communities and individuals to analyze their context and to design their own responses to digital harms are more promising' than 'direct' efforts, such as counterspeech or deleting harmful speech online (D14:Q53). Statements such as this clearly speak of the moral disengagement of actors within the international domain, whose responses are framed as less effective, and the moral engagement of individuals based within (local) communities who are tasked with addressing the negative consequences of digital technologies which have global origins.

The individualization of moral responsibility can bring immediate harm to end users, particularly in authoritarian or politically volatile contexts. To mitigate the physical security risks associated with PeaceTech, a minority of contributions advocate the non-use of digital technologies. Under the heading of 'informed consent', the ethics discourse morally engages end users in the difficult task of deciding 'whether or not to participate' in digital peacebuilding projects (D13:Q1). However, the discourse does not seem to shy away from attributing the moral responsibility of not using technologies to the end users as well. This cascading down of responsibility results from the belief within the international domain that 'since the technology is already there, it would be a pity not to use it to better plan, implement and monitor our programmes' (D27:Q113). Since the use of a technology has already been established further up the cascade, its non-use only hinges

on participants' understanding of the complex and tangible risks involved – something that is recognized as 'one of the most challenging ethical obligations to get right, especially when working with low-literacy or vulnerable populations' (D13:Q68). In contrast, the possibility that a decision in favour of non-use could already have been made higher up in the cascade, for instance, at the planning stages, is recognized only by a small number of contributions. For example, Build Up's intersectional feminist guidance for digital peacebuilding calls to 'always prioritize people's (online) safety and security over ambitions to understand and address marginalization' (D5:Q41).

Of course, the vulnerability of individual end users differs vastly. Staff members of IOs based at headquarters or in the field who conduct remote consultations using a messenger service will face fewer tangible risks than government delegates to a high-level political process or volunteers who contribute to crowdsourcing activities to monitor contested elections. Overall, however, the tendency to individualize moral responsibility means that those agents in the cascade with the least resources at hand may be morally called upon to address those risks that can cause the greatest harm to their physical safety and well-being. This distribution of moral responsibility ultimately creates a scenario where vulnerable end users must either accept tangible risks to themselves or abandon the digital peacebuilding effort, and with it, its goals.

Many examples illustrate how this individualization of responsibility for tangible risks eventually undermines the objectives of preventing the (re)occurrence of violent conflict. In the case of South Sudan, community monitors engaged in a digital conflict early-warning scheme received death threats due to their involvement in the project, which put them in a position whereby they had to self-censor their conflict reports to protect their personal safety.<sup>69</sup> Country-based IT consultants tasked with rolling out mobile applications for early warning avoided travelling to remote areas affected by violence and insecurity, which meant that the system did not provide data from some of the civilian population areas where it was most needed.<sup>70</sup> In Sri Lanka, local social media monitors have described how the work of sifting through endless amounts of violent and graphic content takes a toll on their mental health, which affects their motivation to provide monitoring data to their international partners, such as the UN. One of the organizations eventually decided to discontinue its partnership with the UN due to the extractive nature of the collaboration, which stood in stark contrast to the personal harms experienced.<sup>71</sup>

While a thorough empirical investigation of the effects of the PeaceTech ethics discourse on peacebuilding practices is beyond the scope of this article, these examples plausibly illustrate a scenario in which individual end users based at the bottom of the risk-responsibility cascade have to weigh up whether to reduce tangible risks to their person or to take the risk of maintaining critical functions of the PeaceTech application in question. The choice may not necessarily be so black and white: participants in online consultations or dialogues may decide to participate while withholding information that could compromise their security. However, no matter how these dynamics play out concretely, it is clear that the dereliction of peacebuilding goals is at least made more likely through the decentring of PeaceTech risk, and the responsibility to address them through an ethics discourse that tends to place the responsibility for dealing with structural and systemic risks at the higher levels, and the responsibility for dealing with personal and tangible risks at the lower levels.

## Conclusion

Our analysis has provided a bird's-eye view of the moral claims regarding the use of digital technologies in international peacebuilding. If analysed individually, these promote valuable goals such as justice and empowerment. Still, in sum, they reveal a crucial fallacy in the current discourse on

<sup>69</sup> Focus Group Discussion with Conflict Monitors of an INGO, Juba, South Sudan, 21 November 2022, conducted by Andreas Hirblinger.

<sup>70</sup> Interview, Member of a Peace Committee in Rumbek State, Rumbek, South Sudan, 21 October 2024, conducted by anonymous researcher.

<sup>71</sup> Interview, Staff of Civil Society Organization, Sri Lanka, Batticaloa, 2 February 2024, conducted by Fabian Hofmann.

PeaceTech ethics: the overarching distribution of moral responsibility within the socio-technical networks that constitute digital peacebuilding creates a specific division of labour that increases the chances that the objectives of digital peacebuilding will be abandoned. We have described this as a case of 'decentred dereliction'. Concretely, we have found that the PeaceTech ethics discourse frames risks, suggests responses, and attributes responsibilities unevenly across what we have described as a cascade: moral agents who are part of the international domain mainly deal with abstract and systemic risks, while the further we go down in the cascade, the more moral agents will have to respond to the tangible and personal risks that emerge during their everyday use of technologies. In most cases, the discourse implicitly or explicitly accepts these adverse effects of ICT use and transfers them through the risk-response-responsibility cascade downwards to individual end users, many of whom will be based in local settings characterized by limited resources to respond to risks.

To be clear, we do not wish our analysis to reproduce racist depictions of powerless, conflict-affected communities that need to be saved by their former (post-)colonial masters. However, we also cannot ignore that the colonial past and global inequalities are embedded in digital peacebuilding and the PeaceTech ethics discourse, as they tend to both romanticize and patronize moral agents located in conflict-affected contexts, while reproducing hierarchies of responsibility and vulnerability. Our findings resonate with David Chandler's analysis of localization in peacebuilding as a transfer of responsibility without power.<sup>72</sup> This is not surprising, given that digitally enhanced peacebuilding is not radically different from peacebuilding 'before' digitalization – if such a differentiation makes sense at all.<sup>73</sup> However, as 'peace' is increasingly conjoined with 'tech', digitalization catalyses such arrangements, and technology becomes the object around which the moral reflexes that contribute to its ordering will take shape.

As we have shown, such a cascading of risks and responsibilities through ethics can have very real and relevant consequences. Where individual end users take risks because of goodwill or ignorance, digital peacebuilding interventions risk harming those contributors who commonly struggle to cope with the challenges of living and operating in conflict-affected contexts. And where end users may not be willing to take on such risks, digital peacebuilding will become compromised, less effective, or even dysfunctional, as the most vulnerable groups log out of online conversations, or self-censor their voices. The effects of the PeaceTech ethics discourse may thus well go beyond potential harms to individual end users. They make it more likely that the stated objectives of digital interventions will not be realized because individual users refuse to bear tangible risks. This could happen explicitly, but it is more likely that it will do so through subtle forms of resistance – for instance, the provision of poor data, self-censorship, or a lack of participation. Our analysis of the decentring of moral responsibility at the heart of the PeaceTech ethics discourse thus points to the potential adverse effects of digital global politics for individual end users *and* digital conflict governance more broadly.

Importantly, the significance of our findings extends beyond efforts to prevent conflict and build peace into other fields of IR. To critically engage with the adverse effects of digitalization, some in the discipline have called for a more worldly and politically engaged social science that productively intervenes in world politics by designing, crafting, and making 'international things', with a radically collaborationist ethos.<sup>74</sup> Our analysis points to the challenges of separating the design and use of 'PeaceTech' from the historically grown forms of decentred governance through which this work is done. Paradoxically, the cascading of risks and responses makes it hard to pinpoint who or

<sup>72</sup>David Chandler, *Peacebuilding: The Twenty Years' Crisis, 1997–2017* (Springer International Publishing, 2017).

<sup>73</sup>Andreas T Hirblinger, 'When the digits don't add up: Research strategies for post-digital peacebuilding', *Cooperation and Conflict*, 59:3 (2024), pp. 425–46.

<sup>74</sup>Jonathan Luke Austin and Anna Leander, 'Making International things: designing world politics differently', *Global Studies Quarterly*, 3:4 (2023), p. ksad068.

what should ultimately be held accountable for, and counteract, the decentred dereliction that we can observe in digital peacebuilding. The decentred moral agency produced through PeaceTech ethics is somewhat akin to what Ulrich Beck described as ‘organized irresponsibility’,<sup>75</sup> namely, decision-making processes where attributing cause and effect is no longer possible, and therefore, the question of (ir)responsibility becomes irrelevant. This increases the likelihood that the objectives of digital peacebuilding will be abandoned. Our research has provided the methodological and empirical foundation to elucidate and counter this trend, providing insights that can be employed to promote an awareness of the relational consequences of the many seemingly isolated instances of moral reasoning.

At the same time, the decentred dereliction we observe complicates easy fixes. It may be tempting to call on decision-makers who are higher up in the cascade to take greater responsibility for those risks that are seemingly far apart and localized, yet integral to digital peacebuilding. This would encourage a stronger awareness of the global and systemic factors that condition the tangible risks at the local level, such as digital authoritarianism or low levels of digital literacy, and could lead to a more comprehensive understanding of what digital peacebuilding must entail. However, simply moving the moral responsibility for such necessary amendments further up the cascade would not change the decentred architecture of digital global politics, and would come with the risk of a moral paternalism that may further disempower the end users of digital technologies. To counter this tendency, it seems likewise crucial to involve those who will unavoidably take on tangible risks – i.e. those who collect data or log into online platforms in insecure and conflict-affected places – in processes of moral reasoning that condition the risks and responsibilities they will take on. That said, such a binary of ‘top-down’ and ‘bottom-up’ fixes would not fundamentally challenge the powerful effects of the cascade.

Instead of identifying specific domains within the cascade that should assume more responsibility, it seems more apt to politicize its distribution. A more fundamental shift in socio-technical ordering requires a disruption of the flow of its normative vectors, for instance through individual actors in the cascade who resist to attempts to award them moral responsibility. As their feedback enters the discourse and practice of PeaceTech ethics, risks can be reframed, and responsibilities, which they are unwilling to take on, redelegated and redistributed. Instead of a cascade, this would enable an oscillating distribution of risks and responsibilities, to which all moral agents involved in digital peacebuilding can contribute. Such attempts to change the flow would likely also reduce the moral distance between the top and the bottom of the cascade, creating a sense that the risks inherent in decentred governance affect the socio-technical network as a whole. A detailed elaboration of the practical consequences of reckoning with the manifestations of decentred dereliction in the digital International is beyond the scope of this article. That said, our contribution has been to render the interlinked chains of moral reasoning that underpin global PeaceTech ethics visible, and in doing so, it has nudged the decentred dereliction at the heart of digital peacebuilding into the space of politics. Put differently, our article points to the need to think about the collective design and use not only in terms of collaboration, but also in terms of the necessary politicization of questions of morality that contribute to the socio-technical ordering of global politics.

**Supplementary material.** The supplementary material for this article can be found at <https://doi.org/10.1017/S0260210525101496>.

**Andreas Hirblinger** is a senior researcher at the Geneva Graduate Institute, Centre on Conflict, Development and Peacebuilding (CCDP). His research is concerned with international peacebuilding and especially with how digitalization and new technologies affect knowledge production and power in efforts to end or prevent armed conflict. He was the Principal Investigator of the research project ‘An Apomediated Peace? The Role of Digital Technologies in International Peacebuilding’, funded by the Swiss National Science Foundation. Andreas obtained his PhD from the University of Cambridge.

**Fabian Hofmann** is a doctoral researcher for Technology and Governance at the Department of Humanities, Social, and Political Sciences, ETH Zürich. He was a junior researcher on the research project ‘An Apomediated Peace? The Role of Digital

<sup>75</sup>Ulrich Beck, *Gegengifte: die organisierte Unverantwortlichkeit* (Suhrkamp, 1988).

Technologies in International Peacebuilding'. Fabian Hofmann holds a master's degree in international relations and political science from the Geneva Graduate Institute.

**Kristoffer Lidén** is a senior researcher and research director at the Peace Research Institute Oslo (PRIO). Working on the ethics of international affairs, his research spans the topics of peacemaking, humanitarian action, security politics, and digital technology.