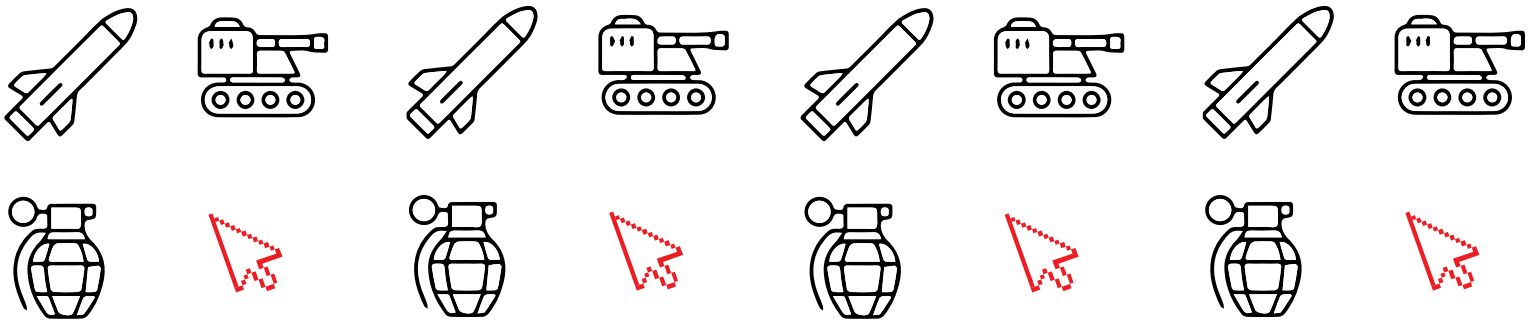
EXPLORING TECH COMPANY RESPONSIBILITY IN ARMED CONFLICT:

An Online Learning Series



ICRC

GLOBAL NETWORK INITIATIVE

GW LAW

sipri

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

Contents

Introduction

Between September and December 2023, the Global Network Initiative (GNI), in collaboration with the International Committee of the Red Cross (ICRC) and the Stockholm International Peace Research Institute (SIPRI), and with support from the George Washington University Law School's Civil and Human Rights Clinic, organized a three-part learning series on the responsibilities of tech companies in situations of armed conflict. This document provides a summary of the series.

The three events that made up this series were each attended by over 65 participants, with 30 participating in at least one session. These participants represented a range of stakeholders including academics, investors, media freedom advocates, and representatives from cloud service providers, digital rights organizations, humanitarian organizations, Internet platforms, technology equipment vendors, and telecommunications companies. The events were conducted under the Chatham House Rule and GNI's Code of Conduct and included break-out rooms and plenary discussions.

The sessions examined a wide range of scenarios and topics, including responsible entry, remain, and exit strategies for tech companies operating in situations of armed conflict. The sessions focused on the importance and implications of international humanitarian law (IHL) and international human rights law (IHRL) for tech companies, their employees, properties, customers, and others in the context of armed conflicts. Much of the discussion centered around identification of approaches to identifying, avoiding, and mitigating conflict-related risks before, during, and after conflicts. In this context, there was also a focus on how tech companies navigate laws and government demands that impact the right to freedom of expression and privacy in such contexts.

The organizers of the series are deeply grateful to all of the participants for their candid contributions and hope that these conversations, and this briefing paper, will continue to help shape critical and collaborative discussion around these important topics.*

*This briefing paper summarizes the discussions during the learning series, and does not necessarily reflect the views of the organizing groups.

Purpose of the Learning Series

The learning series provoked open, honest, conversations about the ways that Information and Communication Technologies (ICT) companies' business activities can have an impact and be impacted in the context of armed conflict. The goal of the workshops was to help ICT companies and other stakeholders improve their understanding of conflict-related risks and improve their ability to make responsible decisions to improve the protection of civilians and others in conflict settings.

Due to the complex nature of armed conflicts, ICTs may offer vital civilian functions in such contexts, but they can also be used for military functions and misused to harm civilians and prolong conflict. Many companies, including ICT companies, approach risk identification and mitigation through the lens of business and human rights, as set out under enduring frameworks such as the OECD Guidelines for Multinational Enterprises, the UN Guiding Principles on Business and Human Rights (UNGPs), and the GNI Principles on Freedom of Expression and Privacy.

However, in armed conflicts, the range of scenarios that companies face can change significantly and quickly. Conflicts involve distinct risks and vulnerabilities for companies, their customers, and others who may be impacted by their activities. Conflict-specific legal rules and standards, in particular under international humanitarian law, that address the unique needs of vulnerable people and populations in such contexts, can apply directly to company personnel and activities. Additional and specific decision-making criteria and risk-analysis tools for operations in conflict settings are needed.

For all of these reasons, and with the backdrop of a number of recent and ongoing armed conflicts around the world, the organizers decided to pool their expertise, resources, and networks to bring this workshop series together.

First Call: September 12, 2023

During the first call, participants discussed issues related to ICT companies conducting business in situations of armed conflict and how they identify, assess, and manage risk to companies, their customers, and others. Many of the participants were familiar with IHRL, as well as IHRL-based frameworks like the OECD Guidelines on Multinational Enterprises and the UNGPs.

The discussion also focused on the rules and principles of IHL, which is a body of international law distinct from IHRL that largely applies only during situations of armed conflict to limit suffering and address conflict-specific vulnerabilities that people and groups of people living in such situations are exposed to.

One of the purposes of this session was to discuss the importance for participants to understand the principles and rules of IHL alongside IHRL so they can better navigate and mitigate risk in situations of armed conflict, including risks of harm to civilian populations and others affected by their operations.

During the discussion, the observation was made that the history of why the rules of IHL came into being can be as important as knowing the specific rules themselves; and that knowing that IHL's aim is to protect civilians and others from the dangers of armed conflict may help motivate ICT companies to align themselves with the protective object and purpose of IHL.

With an already strong foundation in IHRL amongst participants, the discussion focused on emerging issues for ICT companies to be aware of that may arise under IHL when operating in situations of armed conflict. For example, with some governments increasingly relying on ICT companies to support their civilian and military activities, participants discussed how under IHL, company employees and properties are normally considered "civilian" and therefore affords them civilian protections (e.g., they must not be attacked). The group also explored under what circumstances those protections might be lost and the risks that arise if a company employee were to "directly participate in hostilities" or if company property were to qualify as a "military objective."

Second Call: October 17, 2023

The second call in the learning series focused on 'Defining and operating responsibly in post-conflict environments'. While ICT companies are increasingly aware of the risks and responsibilities of operating in conflict settings, less attention has been paid to their role and impact in post-conflict settings. There are many reasons why a company may not consider the impact of its operations in post-conflict contexts. One main challenge is defining a setting as 'post-conflict'.

Given the precarious nature of post-conflict settings and the non-negligible possibility of a return to war, participants discussed how ICT companies in particular must be aware of and prepared for the potential for decisions that they make about their services and activities to be either misinterpreted or actively used by conflict actors to fan or reignite the flames of dispute, conflict, and violence. In such settings, an understanding of the evolving local context is required. Participants discussed how, in many such contexts, there are actors whose interests are, in their own perception and calculations, best served by a continuation of or return to violence. Some participants observed that this is particularly likely to be the case in countries where there is a long-term pattern of the level of violence rising and falling but never quite disappearing.

Overall, the discussion focused on how, in post-conflict settings, companies need to identify a wider range of risks with potentially deeper impacts and consider how to address them proactively.

The responsibility of ICT companies in post-conflict settings

During the session, there was discussion about the importance that when companies operate in a post-conflict settings, they should design their activities with sensitivity to conflict risk – to avoid making the situation worse. At the same time, participants discussed what steps companies can take regarding their products and services so they can contribute to peace processes and foster reconciliation, modulating their activities if necessary to meet the wider needs of that particular market. There was also discussion of what other steps ICT companies can take outside of their normal business practices to the same end. A good example of what this might mean is a systematic engagement with local communities; this not only fosters mutual understanding and avoids potentially dangerous misunderstandings, but it also provides the best basis for analyzing the context.

As set forth in the UNGPs, companies have a responsibility to respect the human rights of all individuals who may be impacted by their products and services. To do this effectively, participants discussed how companies need a capacity for contextual analysis of risk – both risks to the company and risks for the communities in which they operate, including risks that the companies themselves generate or exacerbate. In order to understand those risks, participants observed that ICT companies may need to assess their growing relationship with governments and other political actors; in this context, there was reflection on what neutrality looks like for tech companies, especially those working on information and communications technologies.

Participants also discussed proactive steps that companies can take to support peace and foster stability, while noting that these too can be perilous. It would be beneficial, some participants pointed out, to engage with and learn from local populations when assessing both short-term and longer-term risks, as well as narrowly defined risks to company operations and broader risks to the peace process.

Third Call: December 05, 2023

The third and final workshop in the learning series examined challenges and opportunities that ICT companies and other stakeholders face when operating in pre-conflict scenarios. During the session, participants discussed some of the practices, policies, and strategies that ICT companies and non-company stakeholders have deployed in such scenarios, as well as the difficulties they have faced in doing so.

Session leaders framed the discussion from the outset using the paradigm of "enhanced" or "heightened" human rights due diligence (eHRDD), which is a widely recognized methodology for operating in high-risk/pre-conflict areas.

Within eHRDD, the discussion focused on three key elements of that methodology: conflict sensitivity analysis, industry collaboration, and multi-stakeholder engagement, with breakout groups organized for each element. Participants offered observations and insights ranging from the differential in resources between small and large companies when it comes to dealing with conflict-related challenges, to the proper consideration of exit strategies in extreme situations, taking into account the potential negative human rights impact of any decision. Similar to the discussion in the second session, participants highlighted the importance of engaging with local experts and affected communities while taking into account that such engagement could create security risks if government authorities did not agree with the views of these stakeholders – and that those risks need to be proactively managed and mitigated, in line with a 'do no harm' approach.

Key Takeaways

Throughout the series, participants discussed the benefits of ICT companies comprehending and respecting rules of IHRL and IHL, as applicable, in situations prior, during, and after armed conflict. During the discussion, it was observed that such comprehension and respect was needed to mitigate risks to company employees, properties, customers, civilian populations and others affected by company operations, communities, and other stakeholders. In addition, participants explored the ways in which responsible business frameworks, such as the GNI Principles, the OECD Guidelines, and the UNGPs, provide company-specific guidance that incorporates and builds on rules of international law that protect human rights and prevent harm to civilians and others in times of armed conflict.

The discussions underscored the need for sector-specific risk management approaches within the broader ICT sector. Participants observed that different types of tech companies face distinct challenges in armed conflict settings, requiring tailored strategies to address their specific circumstances.

Emphasis was placed on conflict sensitivity analysis and responsible behavior in post-conflict environments, with participants discussing how tech companies can proactively contribute to peacebuilding efforts while avoiding actions that could exacerbate tensions or reignite conflicts.

Participants explored and unpacked the concept of eHRDD, highlighting conflict sensitivity analysis, industry collaboration, and multi-stakeholder engagement as essential elements for ICT companies operating in pre-conflict scenarios. There was repeated focus on the significance of engaging with local populations and experts to gain a deeper understanding of conflict dynamics and mitigate risks effectively.

Participants emphasized the need for ongoing dialogue and the benefits of using scenarios to explore the rapidly evolving realities that businesses, and civilian populations and others affected by their operations, are facing in armed conflict settings. This continuous engagement could be an avenue for fostering proactive involvement and effective risk management strategies, all to better equip ICTs to respect the rules of IHRL and IHL while operating in such challenging environments.

Such engagement could be based on a collection of case studies, both positive and negative, to facilitate further learning and training to help address abroad range of potential challenges, risks, strategies, and outcomes of operating in conflict-affected and high-risk areas.