GUIDELINES FOR CIVIL SOCIETY ORGANIZATIONS ENGAGING WITH ICT COMPANIES OPERATING IN CONFLICT AFFECTED AND HIGH-RISK AREAS [2024]

INTRODUCTION

Around the world internet freedom and human rights are under siege and digital authoritarianism on the march. Recent years have seen socio-political tensions escalate globally, with a number of regions experiencing violent conflicts. In such conflict-affected and high-risk areas, **civil society organizations (CSOs) play a crucial role in defending the rule of law and promoting human rights online** as well as offline. One challenge for local and regional civil society advocates of internet freedom in such settings is to engage effectively with information, communications, and technology (ICT) companies to promote rights-respecting policies and practices.

Conflict-affected and high-risk areas (CAHRA) are characterized by serious human rights and humanitarian law violations and severe harm to individuals, especially when they involve armed conflict. The ICT sector has a particularly complex nexus to conflict and instability. Digital technologies have become essential features of the day-to-day lives of people and their communities around the globe. At the same time, there is no denying technology's role in exacerbating conflict. The malicious use or disruption of technology to undermine human rights, stability, and security is a growing concern among governments and civil society advocates alike. **The purpose of these Guidelines is to provide local and regional CSOs with a series of insights derived from experience accumulated in the CAHRA context over the past decade, in order to facilitate and strengthen their engagement with ICT companies around human rights and humanitarian law with a focus on issues affecting internet freedom.**

The Guidelines are an integral part of the *Engaging Tech for Internet Freedom* (ETIF) project, a broader initiative spearheaded by ARTICLE 19 that seeks to build capacity among local digital rights organizations in the Asia-Pacific region. Among other things, ETIF seeks to promote many of the international standards reflected in ARTICLE 19's Global Principles on Protection of Freedom of Expression and Privacy. Through research and technical assistance, **ETIF provides local civil society actors with a variety of tools for advocacy *vis à vis* ICT companies operating in countries with authoritarian and repressive regimes. The Guidelines are one such tool, aimed at reinforcing CSO outreach and engagement efforts on the ground.**

Building on the foundation laid by the *UN Guiding Principles on Business and Human Rights* (UNGP) and the pioneering work of organizations such as the Global Network Initiative (GNI), the ETIF Guidelines aim to provide support to **domestic and transnational CSOs operating in the Asia-Pacific region** in conflict-affected and high-risk areas, which are those characterized by a weak or nonexistent rule of law and serious violations of human rights and humanitarian law. As such, the ETIF Guidelines extend the groundbreaking work on business and human rights in the ICT sector previously advanced by experts from the United Nations, GNI, BSR, Internews, and the ICRC, among others.

These Guidelines are divided into three Parts. Each Part covers CSO engagement with ICT companies in one of three scenarios: **(I) conflict-affected and high-risk areas** (CAHRA), *excluding* armed conflict**; (II) during armed conflict**; and **(III) after armed conflict or crisis**. **Users are encouraged to consult the Parts and particular Guidelines most relevant to their operating context.** To this end, they may use the **Overview** that follows to navigate through each Guideline and its sub-parts according to the pertinent scenario and specific context.

PART I: CONFLICT-AFFECTED AND HIGH-RISK AREAS (CAHRA), *excluding armed conflict*

Introduction

This first Part distills much of the wisdom on **Business and Human Rights (BHR) in the ICT sector** already available in prior publications by international and non-governmental organizations and tailors it to the context addressed by the ETIF Guidelines: CSO advocacy for internet freedom with ICT companies in repressive or authoritarian regimes like those in the Asia-Pacific region. It outlines many of the well-established steps recommended by business and human rights (BHR) experts when engaging in outreach to private companies on BHR matters. At the same time, this Part incorporates specific parameters related to the **CAHRA context** in circumstances that fall short of armed conflict. As a result, the approach adopted in these Guidelines, while unique, follows to a great extent the model of **"enhanced" human rights due diligence** (eHRDD) that predominates in this context. In that model, the framework of eHRDD integrates **conflict sensitivity analysis** as well as cross-cutting **multi-stakeholder engagement** across the due diligence process. The next Part examines additional considerations that come into play when a situation of repression or crisis deteriorates to the point that internal or international armed conflict becomes the operational setting.

GUIDELINE 1: Develop an informed strategy for approaching an ICT company operating in Conflict-Affected and High-Risk Areas [CAHRA] and for engaging effectively with its relevant representatives. For a comprehensive overview of this process and the factors involved in carrying it out, *see* BSR's Guide for Civil Society, entitled *Effective Engagement with Technology Companies.*

1. **Define your overall goals strategically and set reasonable expectations for each company engagement activity to avoid frustration and early abandonment of your strategy.**
   - **1.1. Determine the specific objective(s) of each engagement in light of the overall goals** of the partnership.
   - **1.2. Set priorities** with respect to your goals, issues and objectives based on the company to be engaged and the prevailing circumstances.
     - 1.2.1. Look for convergences around issues of mutual interest, i.e. those where the company's interests or priorities align with one or more of the issues you are advocating on.
     - 1.2.2. Seek ways to foster trust and establish constructive relationships with company counterparts.
     - 1.2.3. Take into account past interactions with the company as well as the profiles of the personnel you will have access to in the engagement.
   - **1.3. Be strategic** in how you set your priorities for company engagement in light of the research you carry out on the company (*see* G1- 3 *infra*) and the prevailing circumstances.

2. **Do your homework and be well-informed about local government laws, rules, regulations, and policies that govern the company's operations and that affect the community's human rights**. Keep in mind that companies operate simultaneously within global regulatory and policy structures.
   - **2.1. Understand the local legal system that the company must navigate**. To operate in-country, the company must balance compliance with local laws and adherence to human rights principles.
     - 2.1.1. Examples of local regulations to research include laws impacting freedom of expression (especially expression targeting the government) and data privacy rules, especially those requiring data localization, government access to user data, user data collection (especially without user consent or notification), and suspension of service to users violating the law.
   - **2.2. Understand how international legal standards apply to company operations** under the *UN Guiding Principles on Business and Human Rights*, and their application in conflict-affected and high-risk areas.

2.3. Recognize and highlight discrepancies between domestic law and the pertinent international human rights standards; develop ideas for companies on how to reconcile these inconsistencies in favor of greater human rights protections.

2.3.1. Ensure you possess the expertise not only with respect to domestic law but also on international standards regarding business and human rights and their application in practice.

2.3.2. Consult proactively with other CSOs at the domestic, regional and international levels who have a track record of advising and/or engaging with ICT companies operating in CAHRA.

2.3.3. Participate in multistakeholder initiatives like GNI that promote the responsibility of companies to respect human rights principles, especially where domestic law or practice do not respect them, and that seek to foster corporate best practices in this regard.

3. **Research the target company as well as pertinent personnel; understand its operating landscape to develop an impactful strategy.** Industry and company-specific websites and resources are excellent places to start your research. Specialized CSO databases like those run by Ranking Digital Rights (RDR) and the Business and Human Rights Resource Centre (BHRRC) can provide useful information as well. Researching a company's affiliations with business associations and multistakeholder initiatives (MSIs) can also prove helpful. Finally, open internet searches keyed to companies and/or their personnel will often produce useful inputs.

3.1. To the extent possible, **seek information about any obligations an ICT company may have assumed**, either in their contracts or through external engagements such as business associations or multistakeholder initiatives.

3.1.1. For example, seek information on any human rights requirements written into an ICT company's contracts and advocate for their disclosure in the interest of transparency.

3.2. Identify the "right" people within the company to engage with to further your goals. The right people are those whose responsibilities, priorities or concerns overlap with yours, giving rise to a **convergence of interests.**

3.2.1. Often the "right" people are defined as much by their personal attributes and interests as by their formal position or portfolio within a company,

3.2.2. Leverage any existing relationships (individual or organizational) that you and your colleagues already have**.** Personal and professional relationships can be used to channel constructive outreach in line with these Guidelines.

3.3. Understand that identifying the "right" people to engage in dialogue with is a time-consuming process, with multiple steps:

3.3.1. Research the company structure to determine which departments and team(s) to engage. Companies may have a specific transnational department or team dedicated to business and human rights (BHR) or corporate social responsibility, while others may have a regionally or nationally based team to handle such issues.

3.3.2. Look for departments with personnel who tend to engage with CSOs on policy matters, namely Trust and Safety; Human Rights; Corporate Social Responsibility or ESG; Policy; and Legal.

3.3.3. Identify both potential company stakeholders as well as executive level decision-makers. Focus on winning over the stakeholders and ultimately having them advocate your position to the decision-makers.

3.3.4. If making direct contact with company personnel is difficult, reach out to any business associations or multistakeholder initiatives to which a company belongs to ask for an introduction.

3.3.5. Network! Attend national, regional, and international fora and events in which companies also participate, such as the Internet Governance Forum (IGF) and RightsCon. Look to identify contacts and establish constructive relationships with company representatives.

3.4. Familiarize yourself about the "culture" of the company you want to engage with, especially if it is a foreign transnational company. This means not only paying attention to the nationality of the

company and the personnel with whom you seek to speak, but also the internal corporate culture of the enterprise, and its receptivity to BHR.

3.5. Anticipate and address potential language and other cultural challenges on both sides of the engagement equation. For example, confirm in advance the language to be used when communicating with company representatives. Be aware that meetings with global ICT company representatives are often carried out in English.

3.5.1. Be aware of any cultural factors related to your own CSO that might influence the outreach or engagement.

3.6. Research the company's internal policies and practices aimed at upholding human rights in its operations.

3.6.1. Find out if the company has internal policies in place to implement human rights principles and related contractual or other obligations, and what practices they have developed to apply those policies.

3.6.1.1. Check if the company have a department or personnel dedicated to business and human rights (BHR);

3.6.1.2. If not, check to what extent are human rights matters addressed through the work of other non-specialized departments or personnel.

3.6.2. Investigate the company's products and services and understand the impact they have on human rights. Investigate whether the company has taken steps to carry out human rights impact assessments (HRIAs) for them or plans to.

3.6.3. Investigate how and on what terms the company engages with government authorities, especially with respect to patterns of compliance with official directives that seek to undermine human rights, e.g. on content removal, user data access and surveillance.

3.6.4. Understand the company's stakeholder engagement policies and related opportunities they offer for you to engage with the company on eHRDD and leverage convergence points between their mission and yours.

4. **Conduct a full risk assessment of your engagement strategy before deploying it**. Engaging with companies and carrying out public advocacy on BHR issues can expose CSOs to threats such as government surveillance, as well as intimidation and harassment from both state and non-state actors. CAHRA countries tend to be where these threats are most serious; they are also where tech companies are most reliant on CSOs to help them understand and mitigate the impacts of their products and services. **In all cases, due diligence in risk assessment is required.**

4.1. Prioritize, establish, and implement safety protocols in the lead up and execution of any engagement or consultation plan with ICT companies. Some questions to address include:

4.1.1. What is the nature of the company's relationship to the government? Is it wholly or partially State-owned? To what extent does it do business with the government?

4.1.2. What risk of official or unofficial reprisals is there for reaching out to a company or companies?

4.1.3. What is the background of the company and its personnel with whom you interact? To what extent can you trust them?

4.1.4. Will your outreach put you or your CSO colleagues at risk of reprisal or harm in any way?

4.1.5. Will your outreach activities put others at risk of reprisal or harm in any way?

4.1.6. In light of your ongoing risk assessment process, what measures can you adopt to monitor and mitigate potential risks associated with your BHR outreach strategy? Consider for instance alternative strategies like using "safer" consumer protection law to argue privacy protections.

4.2. Engage ICT companies in the design and deployment of measures to help guarantee your safety and avoid government surveillance during your consultations and after they have taken place.

4.2.1. Keeping in mind Guideline 4.1's safety protocols, encourage the use of secure channels of communication, such as the utilization of VPNs or encrypted messaging systems.

GUIDELINE 2: Establish professional and personal relationships with the company and individual company representatives. Much successful outreach and engagement occurs through the channel of existing relationships between CSO advocates and company representatives with whom they have established contact through professional networking. *See* G1 – 3.2.4, *supra*. Effective engagement is not an adversarial process but a collaborative one.

1. **Engage cordially and constructively with companies**. **Aim to collaborate.**
   - **1.1.** Creating and maintaining a good working relationship with company counterparts is **a goal in itself**.
   - **1.2.** Approach company representatives with **constructive messaging**, especially when critiquing policies, practices, or products. Propose realistic responses and solutions whenever possible.
   - **1.3. Understand the asymmetry in the CSO-company relationship**: **positive change depends on persuading or convincing the company representatives** to take some action. There is no way to coerce a company decision in the context of constructive and collaborative engagement.
   - **1.4. Engage with the "right" people** in the company and keep in mind their roles and limitations. *See supra* G1 - 3.1.
   - **1.5. Assume good faith intentions and openness to ideas**, until there is evidence to the contrary.

2. **Build trust with company representatives.** Once a relationship is established, the importance of building and maintaining trust with company representatives cannot be overstated. Communicate constructively, using respectful and moderate language. Insist on the same from your counterparts. By so doing you:
   - **2.1. Open lines of communication for companies to approach CSO counterparts for consultations** on issues related to their human rights due diligence activities or when the need otherwise arises;
   - **2.2. Increase the opportunity for CSOs to learn about how a company works**, including through off-the-record exchanges of information;
   - **2.3. Expand involvement with other companies through referrals.** By demonstrating your trustworthiness as an expert and stakeholder, a company representative is more likely to recommend you to his or her industry colleagues, which extends the scope and effectiveness of your engagement.
   - **2.4. Confer with company counterparts** about how each of you should publicly refer to your meetings and interactions in press, social media and other communications.

3. **Recognize that your role as local expert and community representative may include helping to educate company counterparts with respect to the realities on the ground.** Being open to and proactive in helping companies understand a crisis, as well as the impact their operations have on the conflict and human rights, is an important role that CSOs can play.
   - **3.1. Offer to participate in ongoing eHRDD processes** to assist companies with the information-gathering, analysis and assessment required to properly evaluate the impact of their BHR policies and practices. The key to access is to take a non-adversarial stance, one that emphasizes partnership and collaboration. *See* G2 - 4 *infra*.
   - **3.2. Provide companies with the information and support needed to advocate for BHR policies and rebut government push-back and abuses**. Companies seeking to implement effective BHR practices in the CAHRA context will likely confront overreach and resistance from state authorities. Such governments generally do not heed CSOs but will listen to and negotiate with companies. This presents an opportunity for mutual support.
     - **3.2.1.** For example, CSOs can emphasize to companies the importance of including protective human rights commitments in their contracts and advise on how to stand on them when engaging with repressive governments.
     - **3.2.2.** CSOs can achieve this through various means, such as including background information on company human rights commitments in press announcements and/or advocating for publication of secondary regulations related to the contracts.

3.3. Seek to engage regularly with ICT companies of all sizes. Two pitfalls of successful CSO-company engagement are a lack of consistency in contact and communications between them; and an overemphasis on the activities of the biggest ICT companies at the expense of smaller corporate actors who may be amenable to outreach.

3.3.1. Communicate proactively with companies of all sizes on a regular basis and encourage them to come to you with problems to resolve in collaboration. Do not wait for the companies to reach out to you!

3.4. Be aware that multinational companies are more likely to be out of touch with local politics and realities than domestic ones. This creates an opportunity for you to provide the expert local knowledge those companies require.

3.5. Note also that local companies might have closer ties to or a dependence on government authorities, thereby increasing the risks associated with CSO engagement with them.

3.6. Use illustrative case studies to give examples of possible solutions to pursue or pitfalls to avoid; these case studies should be based on the experiences of peer companies, which showcase different approaches available for addressing a challenge or issue.

GUIDELINE 3: Become an indispensable and trusted resource for the company by engaging with it on existing eHRDD and HRIA processes, consulting as information sources, and monitoring the company's progress on all fronts. ICT companies implementing BHR policies in the CAHRA context should be conducting "enhanced" human rights due diligence with respect to their products and services, which includes regular conflict, risk, and human rights impact assessments.

1. **If offered the opportunity to participate as a stakeholder in these processes** as part of the company's engagement strategy, **you should:**

1.1. Embrace the importance of local context and the role of subject matter experts. Companies undertaking eHRDD will require expertise on local conditions relating to CAHRA and on the impacts associated with the company's products and services in that context.

1.1.1. CSOs can act as local and regional experts in conflict-affected and high-risk areas, advising a company on how its products and services contribute to or impact an escalating crisis.

1.2. Build trust by actively seeking to engage with companies as credible sources of information, analysis and insight on the affected regions and local communities, the domestic legal context, and the relevant human rights obligations.

1.2.1. Pursue and embrace an active role in the teams that carry out eHRDD. Companies often seek to build collaborative teams with strong local and regional expertise when creating eHRDD systems, conducting conflict-sensitivity analyses, and carrying out human rights impact assessments. They will be looking for reliable CSOs partners who they can trust!

1.2.2. Participate effectively in the multiple opportunities afforded by eHRDD for stakeholder engagement at every stage of the process; foster trust in your role as a constructive and reliable CSO partner. Be available as a resource for companies even outside the formal eHRDD process; this may include being "on call" for issues as they arise or conducting follow-up assessments as needed (for example, after a company has made changes in practice or policy in response to prior recommendations).

1.2.3. Strengthen trust by engaging regularly and work with the company's internal team to assist with their current needs. Companies' human rights obligations include subjecting their crisis response mechanisms to regular independent audits, which trusted outside CSOs perspectives can contribute to.

1.2.4. Engage constructively with company representatives and the other stakeholders consulted during and after the eHRDD processes to further build trust. Take advantage of the opportunity to get involved by offering thoughtful, good faith feedback and acting like external consultants on the BHR issues presented.

1.3. Actively monitor the company's processes at all stages of the eHRDD framework to evaluate, document and report on its progress. Communicate your findings and recommendations to the company constructively, suggesting responses and solutions where appropriate. **Consider public-facing reporting,** depending on the degree of constructive engagement established with the company.

1.3.1. Provide proactive support by recommending strategies that address changing domestic circumstances.

1.3.2. Offer practical recommendations and understand the context in which a company is operating. The more attainable a recommendation the better it will be received. For example, recall that contractual or external commitments may contain constraints that can impact – positively or negatively – a company's ability to address human rights issues. Advocating for transparency in this regard can aid in defense or accountability of company conduct.

1.3.3. Advocate for the company to publish information from its HRDD that will help them show that they have conducted HRDD and inspire other companies to do so.

1.3.4. Give constructive feedback on published information and share good practices. Help the company assess any risks associated with the publication of its assessments.

1.3.5. Be the voice of your community when providing analysis and insights on the potential or actual risks stemming from the company's products, services, operations, or designs.

1.3.6. In extreme cases, CSOs may have a role in facilitating a responsible exit by contributing to conflict and risk assessments by ICT companies of when a partial or full market exit may be appropriate.

2. **In the alternative, where there is a lack of meaningful engagement opportunities within and around company eHRDD processes, consider conducting your own shadow or community-led human rights impact assessments, to produce independent analyses for company and public audiences**.

2.1. Avail yourself of specialized models, methodologies and templates created for just this purpose, in particular **the *Community-led Assessments of Rights Impacts in the Technology Industry* (CLARITI)**, which is designed for CAHRA settings.

2.2. Use alternative HRIAs **to independently evaluate the actual and potential adverse effects** of the company's actions, services, or products selected for assessment.

2.3. Leverage local connections and regional expertise to generate useful information, insight, and analysis regarding the impact of the company's action, service, or product studied, especially with respect to:

2.3.1. The conflict or crisis

2.3.2. The human rights of the affected population

2.3.3. The impact on civic discourse, such as election processes, and

2.3.4. The effect on employees and the responsibilities of third-party contractors.

GUIDELINE 4: Forge and leverage solidarity across non-company stakeholders with similar goals and objectives. Build networks among like-minded CSOs and engage with other stakeholders to advocate for company actions *collectively*. There is force in numbers! Fragmentation and a lack of coordination

among CSOs is a significant obstacle to effective advocacy. It not only reduces the effectiveness of civil society's engagement, it risks working at cross-purposes, as when the priorities of different CSOs conflict, or are publicly in tension with each other. ICT companies often meet with stakeholders in groups, requiring collective coordination among COSs to maximize the impact and effectiveness of their advocacy agendas.

1. **Think broadly and inclusively about non-company stakeholders to reach out to when networking, building alliances, or coordinating.** In addition to advocacy groups and like-minded CSOs, it includes actors like academics and shareholders who may share at least some of the same goals and objectives as your organization.
2. **Coordinate and Organize**: CSOs and their allies can greatly strengthen the impact of their expertise and advocacy by working in concert with other CSOs in **coalitions and networks** that amplify their voices and those from the affected communities they represent.
3. Coordination with other CSOs and stakeholders does not mean you have to present a single voice on all issues.
   - **3.1. It is possible to advocate around a range of legitimate viewpoints**. The key is to coordinate beforehand to ensure that differences of approach or emphasis are identified and managed by the collective before meeting with a company.
   - **3.2.** In cases of irreconcilable differences of opinion or trust among groups of CSOs, and/or where security risks attach, **it may be preferable to recommend to a company that it engage with the different groups separately**.
4. **Coordinating efforts through coalitions and networks** has many beneficial effects, such as:
   - **4.1 leveraging the limited capacity and resources** of most CSOs to maximize the scope of their collective action;
   - **4.2** making **strategic use of individual CSO expertise** to maximize the range and impact of the group's advocacy efforts;
   - **4.3** allowing CSOs to develop **coordinated if not integrated agendas** that avoid conflicts and contradictions, thus facilitating more effective engagement with companies and making the CSOs easier to engage with from a company perspective;
   - **4.4** enabling **CSOs to work with smaller companies that lack the resources of their larger counterparts to share experiences and best practices** developed by the latter.

PART II: DURING ARMED CONFLICT

Introduction

The onset of **armed conflict or crisis will** substantially affect the way ICT companies and CSOs operate in general; it will also alter the landscape of engagement with companies in a number of notable ways. **It is critical that CSOs be aware of the elevated risks involved and take steps to mitigate or avoid them.** On the one hand, the actual or perceived participation by company personnel or CSO members in an armed conflict can have dire consequences for their safety, requiring **heightened risk assessments**. On the other, the normative framework of Business and Human Rights (BHR) shifts during internal or international armed conflict to recognize the **application of international humanitarian law (IHL)** to the belligerent parties, a fact which has important repercussions for how ICT companies – and the CSOs who wish to engage with them – operate. In particular, an understanding by all stakeholders of how IHL shapes the discussion of relevant international standards when carrying out "enhanced" human rights due diligence (eHRDD) becomes essential. CSOs seeking to engage with companies in the context of armed conflict should **prioritize their security** along with that of affected communities whose interest they seek to promote and protect. Similarly, in this context, **conflict sensitivity analysis** – the distinguishing component of eHRDD – will take greater precedence throughout the stakeholder engagement process.

Even in situations of armed conflict, many of the Guidelines outlined in the prior Part will still be relevant, such as the importance of coordinating CSO communications (Part I: Guideline 4); fostering professional and personal relationships (Part I: Guideline 2); pursuing trust-building measures (Part I: Guideline 3); and finding a common language for communication (Part I: Guideline 3.4). Accordingly, this Part will focus on highlighting those dimensions of **CSO engagement** that are unique or of heightened importance **during armed conflict.**

GUIDELINE 1: CSOs should adapt and reinforce their security protocols, including for their members, in response to the escalating conditions of conflict; by the same token, assess and promote the safety of users and communities affected by the products and services of ICT companies operating in armed conflict.

1. **Prioritize the safety of CSO members, infrastructure, and constituencies and implement measures to protect them.** The **ICRC recommends that during armed conflict CSOs:**
   - **1.1. enact strong measures to protect the data they collect and process,** and they should build internal resilience to digital threats against their IT systems and operations;
   - **1.2. prepare to be the target of harmful information** that may affect their operations and reputation, **and be prepared to respond appropriately**, both online and offline;
   - **1.3. develop responses to harmful information against civilians** in their operations;
   - **1.4.** should **strengthen their efforts to raise awareness of the international standards on the protection of civilians** that apply during armed conflict, especially among companies providing digital services, as outlined in the Guideline 3 *infra.*

GUIDELINE 2: Confirm or advocate that companies operating in armed conflict carry out "enhanced" human rights due diligence (eHRDD) that is informed by local experts who can inform the company's conflict sensitivity analyses, risk assessments and other processes as appropriate. ICT companies' products and services, in particular digital platforms, can play a significant role in facilitating harm to the civilian population during armed conflict, for example, through the spread of harmful information or by enabling surveillance. Accordingly, these companies will need to take additional measures to properly assess such risks, ideally with the support of CSOs. In this context, ICT company procedures and practices, including content moderation, should align with IHL and human rights standards.

1. **Ensure that companies have eHRDD policies with not just human rights but also international humanitarian law (IHL) norms in place.**
   - **1.1. Encourage companies to conduct a rapid eHRDD** to identify and mitigate any actual or foreseeable negative impact on human rights and IHL.
   - **1.2. It is important that CSOs understand the basic interplay of human rights and IHL** standards in the context of armed conflict, so as to better engage with their company counterparts on that subject.
   - **1.3. Conflict sensitivity analysis** means companies should be able to **anticipate the escalation of conflict** and the effects such escalations will have on the normative framework and eHRDD processes that will apply **in extreme scenarios**, ideally with CSO inputs and local expertise.
   - **1.4. CSOs should be prepared to engage with ICT companies in the development of such scenarios** and their impact on company BHR policies and practices, and actively seek to do so.
   - **1.5.** One way to do this is to **assist in the development of "carve-out" policies** that activate during times of crisis. Companies' policies and standards are designed for less extreme operating environments, which may make them harmful or counterproductive when enforced in times of crisis or armed conflict.

2. **Assist companies as the exigent circumstances require at every step of the eHRDD process.** It is important to understand that in crisis situations the companies may face a tension between promoting BHR and international principles on the one hand, and obeying local law and/or government orders that are in conflict with those principles on the other. This is especially the case when military actions or civil unrest threaten the safety of company personnel, infrastructure, and operations.
   - **2.1. Recognize that ICT companies will prioritize the security of their personnel, contractors, and suppliers** when operating in conflict-affected areas, especially armed conflict.
   - **2.2. Assist in the development of policies and practices that take into account IHL as well as human rights norms, as appropriate.** Ensure that companies operate with transparency on policy design and enforcement under the circumstances. Encourage companies to make any policy changes clear and communicate those changes publicly.
   - **2.3. Request that companies be transparent and disclose government demands** that may negatively impact the civilian population such as demands for user data, the adoption of surveillance measures, censorship, or the promotion of harmful information, as well as the company's response.

3. **Advise ICT companies to prevent their platforms, services, or products from being used to contribute to human rights and IHL violations and to proscribe users who promote, commit, or contribute to committing, human rights or IHL abuses.** Companies can and should play a role in protecting civilians against the foreseeable harms of cyber and other military operations. **CSOs can and should play a role in helping company stakeholders familiarize themselves with the applicable principles of IHL,** especially **the principle of distinction**, which is founded on the differentiation between military and civilian objectives. For example**, CSOs should urge and assist companies to adopt measures to protect their property and personnel and other civilians by preventing:**
   - **3.1.** inadvertent but direct participation in the hostilities, which can lead to a loss of IHL protections;
   - **3.2.** the spread of information (including disinformation) that endangers or harms civilians;
   - **3.3.** debilitating cyber-attacks on civilian infrastructure or the provision of essential services;
   - **3.4.** the exploitation of commercial digital surveillance that captures personal data, such as targeted advertising, by parties to the conflict.
   - **3.5. ICT companies and humanitarian organizations must work together to identify such digital threats** during armed conflict and find innovative solutions as needed to address them.

4. **Contact companies with constructive feedback on their eHRDD policies in practice, especially regarding IHL protections**. An outcome of effective CSO monitoring of eHRDD processes during armed conflict is the creation of a positive feedback loop for ICT companies that incorporates IHL norms and principles. For example, if a company's impact assessments lack key inputs based on IHL protections, or their mitigations are insufficient in that regard, CSOs can recommend and support improvements in these areas. **To do so, CSOs can:**
   - **4.1. monitor company eHRDD activities** and assessments in support of that process;
   - **4.2.** identify and warn companies of the ways that the parties to a conflict are **utilizing – and especially misusing – their technology during armed conflict,** thus notifying them of potential infractions of IHL and human rights norms;
   - **4.3.** prepare materials demonstrating how **the conduct of the belligerents,** especially the government, is negatively impacting human rights and IHL protections where that is the case;
   - **4.4.** assist companies to develop, implement and monitor **human rights and IHL risk assessments** of both the role and status of their property and personnel during the armed conflict;
   - **4.5. suggest creative solutions** that comply with legitimate government regulation but keep human rights and humanitarian law central to company operations, to the extent possible.

GUIDELINE 3: Advocate with companies for adopting an equitable, fair, and consistent approach to operating in situations of armed conflict and crises, to avoid appearing partisan or being perceived as supporting partisan positions. ICT companies operating in situations of armed conflict must understand that the services they provide may amount to a direct participation in hostilities by their employees and whether the company's personnel or property might therefore legitimately qualify as military objectives.

1. **When engaging with ICT companies during conflict, CSOs should recommend that, to the maximum extent feasible, they take measures to avoid participating directly in the hostilities or harming civilians.** Companies can do so by:
   - **1.1. segmenting data and communications infrastructure** provided for military purposes from that utilized for civilian purposes, and **monitor their services and infrastructure** to avoid participation in the hostilities or the appearance thereof;
   - **1.2. ensuring that measures taken for commercial or other reasons do not impede the functioning, maintenance, and safety of medical services, humanitarian activities, or other services essential to meet the basic needs of civilian populations;**
   - **1.3. prioritizing the allocation of company resources based on salience, scale, and scope of human rights and IHL threats and violations.**
2. **Civil society expects companies to have a standardized and consistent response to crises and conflicts.** CSOs should therefore highlight the expectation that companies address the risks and adverse impacts of their services and products during crises in a systematized and equitable manner.
3. **CSOs should also look to understand how the company may have responded fairly and effectively to recent conflicts in other regions and advocate for similar actions.**

GUIDELINE 4: Be available for meaningful, direct, and concurrent engagement with companies operating in times of armed conflict whether or not it takes place within the eHRDD framework.

1. **Make yourself available for ongoing communication regardless of the context.** When a crisis or armed conflict breaks out, companies are expected to immediately engage with local and regional human rights experts, CSOs, and other relevant stakeholders to advise on and monitor the company's activities and the impact of crisis measures on affected communities.
   - **1.1. Don't wait!** Take the first step and reach out directly.
   - **1.2. Leverage existing relationships** to check in and provide help.
   - **1.3. Ask company personnel for guidance on effective engagement**.
2. **Seek to establish contact with the ICRC which operates in conflict zones across the world.** This expert organization may be able to offer you guidance on how to better engage with companies regarding their obligations and operations under IHL.
3. **Develop partnerships with other CSOs to engage with companies collaboratively in times of crisis and present a unified front in your advocacy.**
4. **Consider creating a dedicated communication channel to monitor updates/requests for engagement.**
   - **4.1.** Companies are also expected to regularly update stakeholders about the ongoing situation and the company's consequent measures and actions.
5. **Be strategic in balancing private conversations and public campaigns**. Be sure to engage with your sectorial partners before public advocacy efforts to respect confidences and maintain trust.

PART III: AFTER ARMED CONFLICT OR CRISIS

Introduction

In the aftermath of armed conflict or crisis, **companies play a vital role in transitioning toward peace and safeguarding human rights**. During this sensitive period, CSOs should actively engage with ICT companies, advocating for gradually winding down conflict-era policies while maintaining proactive measures such as eHRDD and comprehensive human rights impact assessments. The goal is to guide companies towards responsible post-conflict practices, contributing to sustainable peace, justice, and development.

In many respects, the post-conflict phase mirrors the context examined in Part I with respect to conflict-affected and high-risk areas (CAHRA). Accordingly, most if not all of the Guidelines from Part I will be relevant here as well. At the same time, however, **a number of additional considerations are specific to post-armed conflict** or crisis scenarios; those are highlighted in this Part.

GUIDELINE 1: Advocate for a transitional phase before the company stops policies that were active during armed conflict.

1. **Engage with companies to influence and assist in the formation of just post-conflict policies.**
   1.1. Advocate for a metered winding down of policies. Ensure users/customers are properly notified of any change in platform functionalities, based on continuous assessments of the conflict's intensity and life cycle.
   1.2. Encourage the growth of partnerships and improvement to the company's adherence to the UNGPs.
   1.3. Remember that the focus is once again on human rights norms as the parameters for implementing and complying with UNGP obligations.

GUIDELINE 2: Advocate for companies to continue to conduct eHRDD to identify, mitigate, and address negative human rights impacts throughout the lifecycle of conflicts and crises.

1. After the conclusion of a conflict, encourage companies to:
   1.1. conduct an audit to review whether their crisis protocols and procedures were adequately followed and implemented;
   1.2. prepare materials and be ready to participate in feedback solicitation as part of this review;
   1.3. conduct a public, full, and independent human rights impact assessment (HRIA) of their activities throughout the crisis.

GUIDELINE 3: Encourage cooperation with judicial accountability mechanisms, and otherwise support transitional justice initiatives designed to ensure redress and avoid the recurrence of armed conflict.

1. Encourage tech companies to prioritize processing requests to access documentation of potential international crimes and human rights violations for judicial accountability mechanisms.

GUIDELINE 4: Reflect on the effectiveness of measures taken during times of crisis, and how to support conflict reduction policies and practices to avoid relapses.

1. Encourage companies to reflect on whether the policies they utilized during the conflict were effective.
2. Workshop with the company to improve the policies and include community advocates in the meetings to ensure the effects on the community is heard.