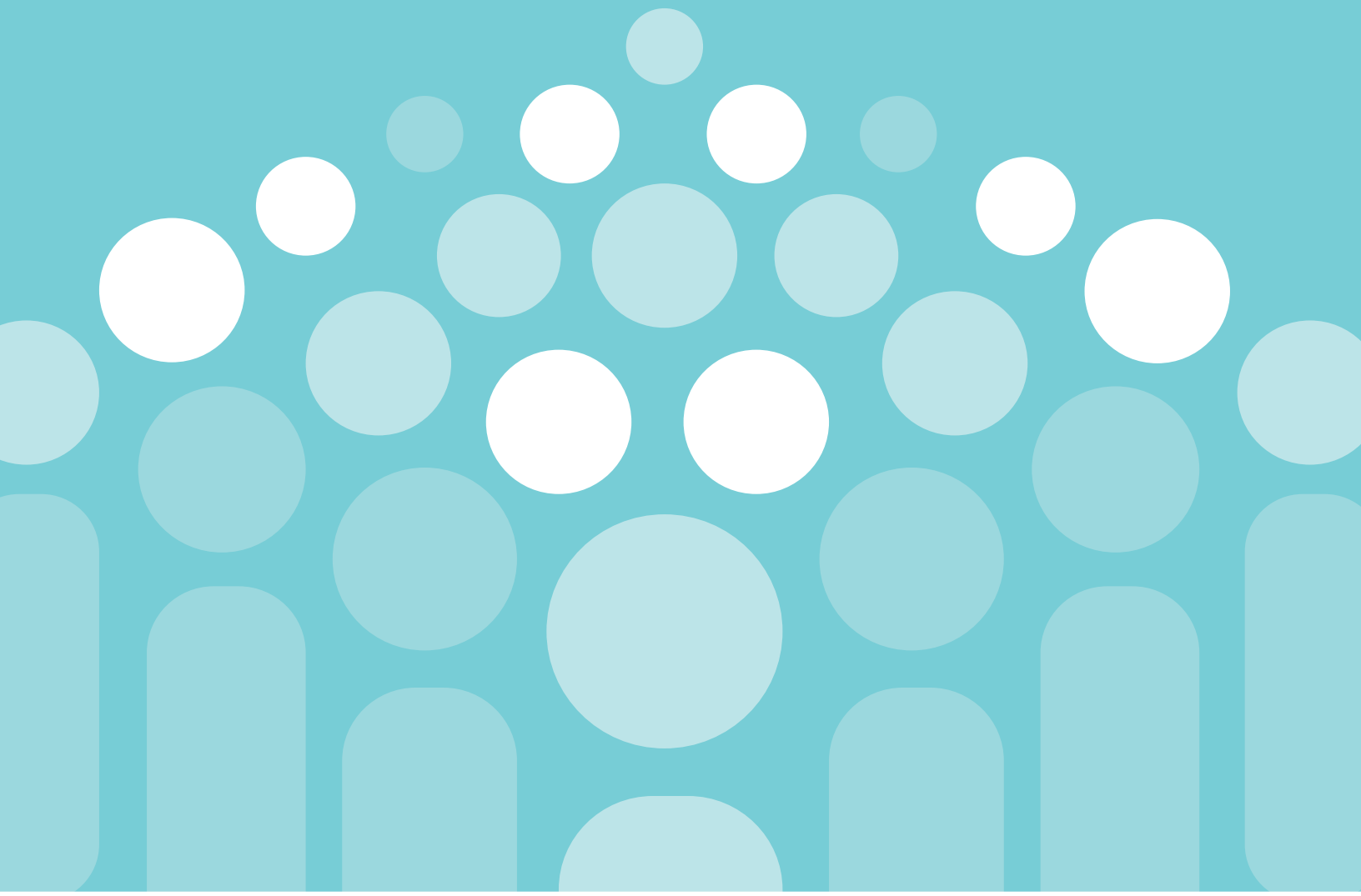

INVESTOR ALLIANCE FOR HUMAN RIGHTS
AN INITIATIVE OF ICCR

HEARTLAND INITIATIVE

SECTOR-WIDE RISK ASSESSMENT:
Information and Communications Technology (ICT)

SALIENT ISSUE BRIEFING:
Conflict & Security

CONTENTS

INVESTOR ALLIANCE FOR HUMAN RIGHTS
AN INITIATIVE OF ICCR

SECTOR-WIDE RISK ASSESSMENT:
Information, Communications and Technology (ICT)

SALIENT ISSUE BRIEFING:
Conflict & Security

The right to life, liberty and security ("security") is a salient human rights issue in the ICT sector. The concept of 'salience' focuses on risk to people, not to the company, while recognizing that where risks to human rights are greatest, such as conflict-affected and high-risk areas, there is significant convergence with business risk.

The ICT sector can promote security and other human rights in conflict-affected areas by helping to amplify the voices of vulnerable communities experiencing conflict, enabling the investigation of abuses through open source intelligence, enhancing peacekeeping/building efforts through crowd-sourcing technology, and assisting in the rebuilding of post-conflict economies. However, the benefits of new technologies can be severely undermined when human rights are adversely impacted by their misuse in ways that escalate conflict. This may include the use of technology to surveil, detain, and/or censor individuals or groups, wage cyber-attacks on civilian infrastructure, "weaponize information" and provide a platform for "hate speech," unlawfully seize property to develop ICT infrastructure, or the sourcing of materials from conflict-affected areas

INTERNATIONAL STANDARDS[1]

Definitions, instruments, and authorities to consider when conducting human rights due diligence in relation to security and other salient human rights issues in conflict-affected areas.

International humanitarian law and human rights law include specific provisions concerning ICT as it relates to security, cyber-warfare, hate speech, land rights, and other salient human rights issues.

The Universal Declaration of Human Rights states that "everyone has the right to life, liberty and security," which is reaffirmed through Articles 6(1) and 9(1) of the International Covenant on Civil and Political Rights (ICCPR). Article 20(2) ICCPR prohibits "Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence." In turn, article 1(1) of the International Covenant on Economic, Social, and Cultural Rights states that "All peoples may, for their own ends, freely dispose of their natural wealth and resources without prejudice to any obligations arising out of international economic co-operation."

In the case of armed conflict, the governing body of law is international humanitarian law (IHL), while internationally proclaimed rights also apply during situations of conflict or widespread violence. IHL, like ICCPR, expressly prohibits the killing of civilians and the arbitrary deprivation of liberty. IHL also includes a range of prohibitions against discrimination based on race, color, religion, sex, birth, wealth, or any similar criteria and contains specific provisions prohibiting the unlawful seizure of resources, including land that might be used for ICT installations.

[1] This briefing provides a high-level overview of the main human rights instruments and adverse impacts of the ICT sector in conflict-affected areas. It does not encompass each human rights issue and binding legal provision relevant to the activities of the ICT sector in these contexts.

Where the use of cyber capabilities in armed conflict is concerned, the International Committee of the Red Cross (ICRC) has, since 2011, affirmed that companies must comply with all the rules of IHL, as is the case with any other weapon, means, or method of warfare. In this same vein, the NATO Cooperative Cyber Defence Centre of Excellence has released two versions of the *Tallinn Manual*, which examines IHL governing cyber warfare.

Lastly, the UN Guiding Principles on Business & Human Rights call on companies to act with enhanced due diligence in conflict-affected areas, where the risks of causing or contributing to gross human rights abuses are particularly high.

HOW DO ICT COMPANIES IMPACT CONFLICT AND SECURITY IN PRACTICE?

In a 2015 special issue of the Journal of Peace Research – "Communication, technology, and political conflict" – 17 scholars found that the introduction of new technologies is typically accompanied by increased political violence and state capacity for repression. Reflecting on the impact of ICT on conflict, the ICRC notes: "Whilst major conflicts are mainly happening in the physical world with kinetic power, new technologies are rapidly giving rise to unprecedented methods of warfare and digital risks."

ICT can negatively impact the right to security and other salient human rights issues in conflict-affected areas in numerous ways, including:

- Enabling governments engaged in conflict to surveil, detain, torture, and in some cases murder, human rights defenders, journalists, lawyers, and dissidents (e.g., Qosmos case in Syria);
- Providing a platform for governments and/or armed groups to "weaponize information" and disseminate "hate speech" against vulnerable communities (e.g., Facebook used to incite violence against Rohingya minority in Myanmar, ISIS in Syria /Iraq);
- Using cyber-attacks against a country's civilian and government infrastructure by another state or non-state armed group (e.g., cyber-attacks by Russia against Georgia's Internet and government agencies during the 2008 armed conflict);
- Constructing ICT infrastructure on occupied land (e.g., Israel in the West Bank, e.g. Hot Telecommunication Systems) and the taking over of occupied population's ICT infrastructure by occupying powers (e.g., Russia in Crimea, e.g. Ukrtelecom);

RESOURCES

- Authoritarian Tech provides global reporting on how governments abuse and distort the power and potential of emerging technologies.
- Global Network Initiative helps companies respect freedom of expression and privacy rights when faced with government pressure to hand over user data, remove content, or restrict communications.
- Institute for Human Rights & Business and Shift provide guidance on implementing the UNGPs in the ICT sector.
- Myanmar Centre for Responsible Business provides a comprehensive ICT sector-wide impact assessment in Myanmar.
- NATO Cooperative Cyber Defence Centre of Excellence and ICRC analyze the ways that IHL governs cyber warfare in conflict.
- Shared Space Under Pressure: Business Support for Civic Freedoms and Human Rights Defenders provides guidance for ICT companies on supporting human rights defenders and the digital space in conflict-affected areas.
- Stanford Global Digital Policy Initiative helps establish norms and policies to enhance the benefits of technology for the exercise of universal human rights, while protecting against the risks for personal, national and international security.

continued on next page

- Providing support to state or non-state armed groups, which illegally control territory or sources of natural resources in conflict zones (e.g., e.g., cobalt mining in DR Congo);
- Sourcing raw materials from conflict-affected areas characterized by child and forced labor, sexual violence, and other labor rights abuses; and
- Providing online platforms for businesses operating unlawfully in conflict zones to market themselves or otherwise engage with global value chains (e.g. extractive industries, factories or service providers in occupied territories).

- The Wassenaar Arrangement promotes transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies.
- Investor Obligations in Occupied Territories: A Report on the Norwegian Government Pension Fund, provides a resource for investors on human rights due diligence for portfolio companies operating in occupied territories.

Business & Human Rights Resource Centre

Between 2014 and 2018, Business and Human Rights Resource Centre (BHRRC) surveyed 68 ICT companies for allegations of human rights abuses. 38 percent of the allegations involved violence and oppression (including the surveillance, detention, torture, and murder of dissidents), 5 percent were related to security issues and conflict zones, and 5 percent were related to land rights and forced displacement.

How does Artificial Intelligence impact conflict and security?

Companies' design, use and deployment of Artificial Intelligence (AI) have significant impacts on security and other salient human rights issues, especially in conflict-affected areas. Algorithmic content moderation can enhance "sensational" content, which often involves extremist views, as well as incitement to and organization of violence by governments and non-state armed groups. It can also accelerate the spread of "fake news" and disinformation – especially with the rapid development of "deep fakes" – putting already vulnerable communities in conflict at greater risk.

In addition, governments, especially authoritarian regimes, can use AI-enhanced technology for selective and retroactive censorship through predictive control of potential dissidents. AI-enhanced surveillance, such as facial recognition, increases mass surveillance and can lead to physical harm including detention, torture, forced disappearances, and killings. Governments have also expressed interest in using facial recognition to track specific groups, such as human rights defenders, migrants, or religious minorities. Overall, such technologies seriously intrude on people's right to liberty. Moreover, AI-enhanced and autonomous weapons (so-called "killer robots") contribute to harming or killing people.

Finally, algorithmic-driven instruments for predictive decision-making, such as risk assessment tools in pretrial detention, predicting crime "hotspots" for allocating police resources, or the integration of private social media data with public databases, can lead to arbitrary detention, thereby impacting people's right to liberty and security.

THE 'BUSINESS CASE' FOR CONFLICT AND SECURITY

Beyond their human rights responsibilities, ICT companies that do not proactively identify, assess, and address security and other human rights in conflict-affected areas face potential legal, reputational, and financial risks.

In conflict-affected areas, characterized by gross and widespread human rights violations, salient human rights risks often translate into material risks for companies and their investors. "Conflict risk" is now the leading ESG criteria among institutional investors according to the US SIF 2018 Trends Report. Conflict is also high on the regulatory agenda of States and multilateral institutions – against terrorism and corruption and towards enhanced transparency, such as the Global Magnitsky Act and EU guidelines on non-financial reporting. ICT companies that do not adequately identify and address adverse risks and impacts linked to security, hate speech, land rights, raw material sourcing, and other human rights issues in conflict-affected areas may face legal liability, erosion of trust and brand damage, and divestment, all resulting in additional expenses and financial loss. Similarly, ICT companies that do no not properly vet contracts with governments engaged in conflict risk regulatory enforcement, shareholder action, and employee protest.

HUMAN RIGHTS GUIDANCE FOR BUSINESS ON CONFLICT AND SECURITY

Drawing from the ICT Sector Guide on Implementing the UNGP, the United Nations Cyberspace and International Peace and Security report, the *Tallinn Manual* on the International Law Applicable to Cyber Warfare, and relevant provisions of IHL and human rights, the following human rights due diligence guidance for businesses to prevent, mitigate and address adverse impacts on security and other human rights issues in conflict-affected areas helps inform investor engagements with ICT companies.

Companies should recognize that the global standard for ensuring right to life, liberty, and security is IHL in armed conflict and human rights law at all times.	Companies should, at the highest levels of leadership, adopt and publicly disclose policies that direct all business units, including local subsidiaries, to abide by IHL in conflict-affected areas and resolve legal ambiguity in favor of respect for the right to security and other human rights.
Companies should clearly identify and prioritize real and potential adverse impacts to security and other salient human rights issues associated with their operations, products, and/or services in conflict-affected areas.	This includes risks associated with the curation of user feeds and other forms of content delivery leading to violence; technology that enables mass surveillance, and AI-enhanced and autonomous weapons. There should be board-level oversight of how the company's business operations are conducted in conflict-affected areas.
Companies should commit to pushing back against excessively broad or extra-legal third party requests that may impact individuals' security, including requests from governments engaged in conflict.	When faced with problematic requests, companies should seek clarification or modification; request the assistance of civil society, peer companies, relevant government authorities, international and regional bodies, and other stakeholders; and explore all legal options for challenge, to protect the identity and security of the user.

Companies should have in place clear and detailed content moderation policies and processes to prevent viral spreading of hate speech, incitement to violence, and other types of "weaponized information."	This includes "sensational" content, extremist views, hate speech, disinformation and fake news, which can incite or exacerbate conflict and lead to offline violence. Efforts should include strengthening human evaluation of flagged content, and providing users with accessible and meaningful opportunities to opt out of platform-driven content curation.
Companies should decline contracts with governments and non-state armed groups involved in conflict to develop or sell AI-enhanced weapons.	This include tools for individual and mass surveillance, and risk assessment tools for pretrial detention, especially when there are no strong safeguards protecting users' security. It also includes AI-enhanced and autonomous weapons that can be used against civilians in armed conflict.
Companies should ensure that land and other resoures used to develop ICT infrastructure have been obtained in accordance with IHL and human rights law.	This includes obtaining free, prior, and informed consent from indigenous communities; ensuring that infrastructure is not developed on occupied land without the consent of the occupied population or for purposes othen than the occupied population's benefit; and not developing infrastructure on land in which vulnerable communities have been forcibly displaced and/or not been adequately compensated.
Companies should ensure that their supply chains are not implicated in human rights abuses or in other practices leading to the escalation of violence in conflict-affected areas.	This includes conducting enhanced human rights due diligence and requiring suppliers to conduct enhanced due diligence to ensure raw materials and hardware are not being sourced in a manner involving sexual violence, child/forced labor, human trafficking, labor rights abuses, and other human rights abuses in conflict-affected areas.

Multi-stakeholder engagement to ensure respect for human rights in conflict-affected areas

Businesses should seek to collaborate with other stakeholders to prevent and address real and potential human rights abuses in conflict-affected areas. For example, in response to the violence committed against the Rohingya Muslims in Myanmar, and concerns raised by civil society about the company's role in enabling associated abuses, Facebook hired non-profit BSR to conduct an independent human rights impact assessment and committed to taking measures to mitigate risks of violence. Also, in 2018, Google executives declined to renew a military contract with the U.S. government after significant protest among employees over the development of warfare technology. Most recently, Microsoft has been vocal about the need to regulate facial recognition. In any case, effective support of civil society requires cultivating strong relationships with advocacy groups, academics, attorneys and other stakeholders seeking out advice on strategic and effective ways to comply with IHL and human rights across complex value chains in conflict-affected areas.

INVESTOR GUIDANCE FOR ENGAGING ICT COMPANIES

The following questions are intended as a starting point for investors engaging with ICT companies to help them evaluate if companies are meeting their human rights responsibilities and IHL obligations in conflict-affected areas.

Human rights commitment and governance

- Has the company adopted a public facing policy commitment to respect human rights, including the heightened risks associated with conflict-affected areas?
- Does board membership include people with expertise on human rights, including business impacts on conflict, and does the company provide clear evidence of senior-level oversight of conflict risks?

Embedding commitment internally

- Does the company conduct enhanced due diligence, including human rights impact assessments, on a regular basis to respond to changing circumstances in conflict-affected areas? If yes, are these assessments gender-sensitive and do they include meaningful consultation with affected rights-holders?
- Does the company have a policy on developing and deploying AI-powered tools in a manner that is consistent with IHL and human rights standards? Do engineering teams responsible for developing AI tools have expertise in IHL and human rights?

Embedding commitment in relationships

- Does the company's supplier code of conduct require suppliers to conduct human rights due diligence to ensure that it does not source raw materials or hardware involving forced or child labor or conflict financing?
- Does the company have safeguards against potential misuse of its technology by non-state actors (e.g., armed groups), including limiting risks of radicalization and facilitation of organized crime and terrorism? Does it have safeguards against the potential misuse of its technology for "weaponized information" and "hate speech?"
- Does the company offer end-to-end encryption or anonymity options? If so, does the company take measures to balance tensions between its responsibility to ensure privacy and freedom of expression and opinion as well as security and public safety prerogatives? Does the company push back against governments' requests to create "back doors"?
- Does the company take measures in conflict-affected areas to ensure ICT projects are not being built on land that was unlawfully appropriated through forced displacement and/or without adequate compensation?
- Does the company engage with industry peers to drive shared requirements of business relationships, including with governments engaged in conflict and/or entities based in conflict-affected areas?

Disclosing how salient human rights issues are addressed

- Does the company disclose information on its policies and practices regarding collection, use, sharing, and retention of information that could be used to identify, profile, or track its users? Does it disclose how it handles all types of third-party requests (by authorities or any other parties) to share user data, restrict content, restrict access, or shut down service (including network shutdowns by telecommunications companies)?

Ensuring access to remedy

- Does the company offer accessible and effective grievance and remedy mechanisms, allowing employees, users and other potentially affected rights-holders to notify the company when their security or other human rights have been affected or violated in connection with the company's business? If yes, do these policies effectively provide remedy when impacts do occur?

INVESTOR EFFORTS

Investors are taking steps to prevent and mitigate adverse impacts on conflict and security by holding ICT companies accountable. Here are some examples:

- In 2016, Wespath Investments and Benefits, the largest faith-based pension fund in the United States, developed a Human Rights Guideline that identifies and evaluates human rights-related risks in conflict-affected and high-risk areas. Relatedly, the Evangelical Lutheran Church of America and The Episcopalian Church voted to develop "human rights screens" to manage these risks in Israel-Palestine and across the globe.
- In February 2017, a global group of investors representing more than $3.75 trillion in assets under management issued a statement defending the "conflict mineral" reporting requirement of the Dodd-Frank Act in opposition to a planned rollback of the requirement, noting "Conflict minerals disclosure is material to investors."
- In 2018, Danish fund MP Pension divested $60 million in state bonds from countries (and state-affiliated companies) responsible for violating human rights, often during the course of armed conflicts.
- In June 2018, a group of 47 institutional investors representing $1.2 trillion in assets issued a statement cautioning companies to continue to comply with the conflict minerals reporting requirements legislated in section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protections Act, which requires them to file annual reports.
- In May 2018, a coalition of over 70 Facebook investors, civil and human rights organizations, and privacy and technology groups wrote to the CEOs of the company's largest institutional shareholders to establish adequate corporate governance on urgent human rights issues, including the use of Facebook to disseminate hate speech against the Rohingya in Myanmar.
- In late 2018, a coalition of shareholders sent an engagement letter and subsequently filed a shareholder resolution with Booz Allen Hamilton expressing concern over the consultancy firm's contract with the Kingdom of Saudi Arabia, including in part its role in the training of the Kingdom's "growing ranks of cyber-fighters."

INVESTOR ALLIANCE FOR HUMAN RIGHTS
AN INITIATIVE OF ICCR

The **Investor Alliance for Human Rights** is a collective action platform for responsible investment that is grounded in respect for people's fundamental rights. Along with civil society allies, we equip the investment community with expertise and opportunities to put the investor responsibility to respect human rights into practice. We do this by: (1) providing tools and resources for investor action on human rights, (2) supporting direct engagement with portfolio companies on their own human rights practices, and (3) coordinating advocacy that asks policy-makers and standard-setting bodies to create level-playing fields for responsible business. Our members are based across four continents and represent $3.5 trillion assets under management. Our diverse membership includes asset managers, public and private pension funds, trade union funds, faith-based organizations, foundations, and family funds. The Alliance is an initiative of ICCR. Visit our website at: https://investorsforhumanrights.org and follow us on Twitter: @InvestForRights

Developed by the Investor Alliance for Human Rights and Heartland Initiative.