


REPORT

Human rights due diligence in the global defence industry

Lessons from other sectors

A close-up, black and white photograph of a hand holding a bullet. The bullet is held between the thumb and index finger, pointing upwards. The background is a dark, textured grey.

Boris Verbrugge
Didier Verbruggen
Hans Merket

flemish
peaceinstitute

REPORT

Human rights due diligence in the global defence industry: Lessons from other sectors



Colophon

Human rights due diligence in the global defence industry: Lessons from other sectors

© Flemish Peace Institute, Brussels, January 2025

ISBN: 9789464074307

Authors: Boris Verbrugge, Didier Verbruggen and Hans Merket

Editing: John Linnegar

Printing: artoos group

Publisher: Nils Duquet, Leuvenseweg 86, 1000 Brussel

Disclaimer

Although the Flemish Peace Institute has taken the utmost care in editing this document, it cannot be held liable or responsible for any errors or omissions. Moreover, no liability shall be accepted for any particular use of this document by a reader.

CONTENTS

List of abbreviations	4
Executive summary	6
Introduction	10
1 Understanding due diligence	12
1.1 Due diligence standards	12
1.2 Due diligence rules	14
1.3 (Downstream) due diligence: challenges for corporate practice	16
2 (Downstream) due diligence in the defence industry	19
2.1 Financial, regulatory and legal incentives for exercising human rights due diligence	19
2.2 Existing practices	21
3 Lessons from other sectors	24
3.1 Identify and assess impacts	26
3.2 Taking action to prevent or minimise impacts	31
3.3 When things go wrong: remediation	40
3.4 Tracking the effectiveness of actions	41
3.5 Communicating due diligence	45
3.6 Policy integration	47
Conclusion	50

List of abbreviations

3TG	Tin, tantalum, tungsten and gold
AIA	Aerospace Industries Association
ASD	Aerospace, Security and Defense Industries
ATT	Arms Trade Treaty
AWDC	Antwerp World Diamond Centre
B2B	Business-to-business
BHR	Business and Human Rights
BSR	Business for Social Responsibility
CAHRA	Conflict-affected and high-risk area
CAR	Central African Republic
CFSI	Conflict-free Sourcing Initiative
CMOC	China Molybdenum Company Limited
CoC	Code of Conduct
CSP	Conference of States Parties
CSRD	Corporate Sustainability Reporting Directive
CS3D	Corporate Sustainability Due Diligence Directive
DAP	Downstream Assessment Program
DII	Defense Industry Initiative
DRC	Democratic Republic of the Congo
ESG	Environmental, Social and Governance
ESRS	European Sustainability Reporting Standards
EU	European Union
EY	Ernst & Young
FCA	Fair Cobalt Alliance
GRI	Global Reporting Initiative
GVC	Global Value Chains
G7	Group of Seven
HPE	Hewlett Packard Enterprise
HRDD	Human rights due diligence
IBM	International Business Machines Corporation
ICP	Internal Compliance Program
IFBEC	International Forum on Business Ethical Conduct
IRMA	Initiative for Responsible Mining Assurance
ITUC	International Trade Union Confederation
KP	Kimberley Process
KYC	Know your customer
MSI	Multi-stakeholder initiative
NGO	Non-governmental organisation
OECD	Organization for Economic Co-operation and Development
RBA	Responsible Business Alliance
RJC	Responsible Jewellery Council
RMAP	Responsible Minerals Assurance Process
RMI	Responsible Minerals Initiative

RSBN	Responsible Sourcing Blockchain Network
SME	Small and medium-sized enterprise
UN	United Nations
UNGPs	United Nations Guiding Principles on Business and Human Rights
US	United States
WSR	Worker-driven social responsibility

Executive summary

Pressure is growing on businesses to implement human rights due diligence (HRDD) in order to identify, mitigate and communicate the (potentially) negative impacts of businesses on human rights. In addition to pressures from civil society, clients and investors, businesses are increasingly having to adopt the due diligence requirements that are being integrated into binding legislation on sustainability reporting (CSRD) and due diligence (CS3D). The defence industry in particular has long operated under the assumption that government regulation and voluntary action in the field of arms control would suffice. However, these initiatives fall short of what is required according to international due diligence standards and in terms of the emerging legislation.

Defence companies face important challenges when attempting to implement HRDD, due to the opacity of the arms value chain and also the fact that the most severe risks are situated downstream, being associated with the (mis)use of weapons. Yet defence companies are not the only ones facing challenges. In this report, we explore the ways in which companies in three other sectors (technology, diamonds and non-energy extractives) are trying to deal with similar challenges. Our analysis is structured according to the due diligence processes that were identified in the OECD's due diligence guidelines, which are universally recognised as the "source code" for due diligence by both companies and legislators. Specifically, these guidelines outline six parallel processes:

1 Identifying and assessing impacts

The technology sector in particular provides some clues on how downstream risks can be identified and assessed. Companies such as the tech firm Ericsson are quite advanced in integrating the downstream segment of their value chain into the risk identification and assessment phase. Specific guidance has been developed for this purpose by consultancy firms such as Business for Social Responsibility (BSR); and the American Bar Association's Center for Human Rights has even developed due diligence guidance specifically tailored to the defence industry.

2 Taking action to mitigate impacts

Based on an analysis of emerging practices in other industries, several mechanisms could be identified through which potentially negative impacts can be prevented or mitigated:

- *Contractual leverage*: this involves integrating human rights safeguards into sales contracts, licensing and service agreements, warranty documents, etc. Companies in the tech industry, such as HPE and Ericsson, have integrated human rights policies into their sales processes. Similar practices in the defence industry – such as regulatory, non-re-exportation and hardship clauses – could be expanded further by drawing on tech-sector examples.
- *Integration*: this entails integrating human rights safeguards into sales contracts, licensing and service agreements, warranty documents, etc. While already effective in the defence industry through mechanisms such as mandatory regulatory clauses, non-re-exportation clauses and hardship clauses that account for sanctioning regimes, companies in other sectors, such as tech (e.g., HPE and Ericsson), have also integrated human rights policies into their sales processes. A further, yet largely theoretical, step could involve choosing the applicable law for contracts which aligns most closely with human rights protection standards, possibly incorporating references to UN or OECD Business and Human Rights (BHR) Guidelines.
- *Working with business partners*: many companies facilitate training with sales partners on topics such as business ethics and compliance. Basic training on human rights or responsible product use could be integrated into these modules, and could include practical guidance on identifying clients or sales with heightened human rights risks.
- *Engaging external experts*: the use of auditors and consultants in HRDD is very common, but it presents challenges. Owing to the primarily qualitative nature of human rights auditing, expertise is critical, but the field is still in its infancy. The consulting practices of the “big four” have faced criticism for their narrow focus on compliance. Smaller “boutique” consultancies could provide specialised knowledge, but could prove to be reluctant to engage with arms companies.
- *Industry and multi-stakeholder initiatives (MSI)*: (cross-)sectoral initiatives effectively generate economies of scale and facilitate mutual learning. Multi-stakeholder models add legitimacy and credibility to such initiatives by engaging governments and civil society organisations, as has been happening in the extractives sector and the tech industry. Key considerations include tailoring the OECD Guidelines to the defence industry, appointing a secretariat to manage operations, and ensuring credible, impartial, and transparent monitoring of HRDD measures.

3 Monitoring the effectiveness of actions

Companies in the sectors we have examined commonly rely on auditors to verify the compliance of business partners with human rights standards. In addition, we are seeing a proliferation of digital platforms and tools to track products through global value chains (often using blockchain). This report highlights a number of caveats that

are connected to both practices, which include methodological challenges related to measuring and monitoring human rights and also the fact that they have mostly been applied in an upstream context.

Whereas companies in the defence sector are already turning to technological solutions to resolve problems with compliance and for “know-your-customer” (KYC) screenings (e.g., Orbis), these tools are not (yet) integrating human rights considerations – although steps are being taken in this direction. As in other sectors, there is a healthy degree of scepticism among defence companies about the problem-solving potential of digital tools, summarised by the adage “rubbish in, rubbish out”.

4 Communicating due diligence

Under new EU reporting rules, large defence companies will be expected to report on how their business model has an impact on different sustainability topics. One of these topics specifically relates to impacts on communities. First, companies will have to assess whether the sale or use of their goods could negatively influence aspects such as security, privacy or freedom of expression. Second, companies will have to disclose the policies, activities and targets they have in place to manage these impacts. Third, companies have to disclose information about the due diligence processes they have in place to monitor and resolve negative impacts continuously. While in theory they could disclose that they are not undertaking due diligence, given the sensitive nature of the industry such an approach would be difficult to sustain in practice.

5 Policy integration

According to international due diligence standards, companies should have clear commitments from management, appoint responsible staff, establish formal due diligence policies and processes, and communicate these policies effectively. While some major defence companies are putting in place human rights policies, not all of these policies are yet publicly available, and references to the UNGPs or OECD Guidelines remain limited. As societal and investor expectations grow, defence companies are increasingly seeking to adapt. They can look to sectors such as food retail, where large supermarket chains are moving towards integrated due diligence strategies.

6 Remediation

Finally, there is the question of remediation, or the efforts that companies can or should make to “right the wrong”. When a business is directly involved in causing or contributing to negative impacts on human rights, it has a clear responsibility to remediate the harm or contribute to its resolution. In most cases, however, defence companies are not those causing the harm. Instead, it is clients (and clients of clients) who may be misusing their goods. Whereas due diligence standards such as the UN Guiding Principles recognise that, in such cases, companies do not have a strict obligation to contribute to remediation, it could still be a sensible thing for them to do. For the arms industry, the issue of remediation raises a critical question: Since arms are designed to harm, what does corporate accountability entail in this context? This

unique challenge necessitates further reflection on the extent and limits of companies' responsibilities in dealing with such issues.

Introduction

Human rights has long been a voluntary self-regulatory issue for corporations. Over the past decade, this has begun to change, though, and companies are increasingly being expected by legislators, investors and customers alike to exercise due diligence by identifying and responding to human rights impacts throughout their global value chains. As a result, the concept of due diligence, which is firmly embedded in soft law (notably the UN Guiding Principles on Business and Human Rights (UNGPs)¹ and the OECD Guidelines for Multinational Enterprises²), is progressively being incorporated into hard law. A new milestone was reached in March 2024, when EU negotiators achieved a compromise on the Corporate Sustainability Due Diligence Directive (CS3D), which is intended to make due diligence mandatory for large companies operating in European markets.

In a previous report, the Flemish Peace Institute highlighted the critical need for defence companies to conduct robust due diligence to identify and mitigate downstream risks, and the challenges they may face in this regard.³ These hurdles are inherent in the distinctive nature of the defence sector, which is characterised by the intersection of national security imperatives, complex regulatory frameworks, dual-use technologies, security threats, limited transparency and heightened ethical, legal and humanitarian considerations.

In addition to a growing body of literature on the topic, responsible business conduct received significant attention at the 2023 and 2024 Conferences of States Parties (CSP) of the UN Arms Trade Treaty (ATT). The 2023 final report⁴ welcomed the UNGPs and urged further discussions on their application alongside human rights and international humanitarian law in the context of the Treaty. While the defence industry clearly faces important challenges in implementing due diligence, it is certainly not unique in this predicament. Rather than justifying the curtailment of due diligence obligations, these challenges underline the importance of a tailored approach. In the light of this, analysing practices and lessons learned from other industries can provide valuable

insights for advancing discussions on HRDD in the arms sector. This report explores the possible outline of such an approach, building on these insights.

Concretely, this study sheds light on the ways in which companies in three selected sectors – the technology, diamond and non-energy extractive industries – are attempting to meet the due diligence challenges in more and less effective ways. We chose to focus the analysis on these sectors because they share a number of characteristics with the defence sector or because they have made progress in finding solutions to similar challenges faced by defence contractors. Through this analysis, we want to be able to identify ways forward for the arms-producing and -exporting industry in successfully implementing due diligence.

The production of this report followed a phased approach. In the first phase, we conducted a thorough review of the relevant academic literature and secondary sources – including NGO reports, reports by international organisations and news articles – with the aim of understanding emerging due diligence practices in the three other sectors identified. This literature review was further enriched by a small number of exploratory interviews with experts on arms export controls and conflict minerals, including representatives from NGOs and policy institutions. The entire exercise was made easier by the authors' extensive personal experience in analysing and supporting the implementation of due diligence across various industries.

In the next phase, a panel of experts provided feedback on a preliminary draft of the report during an online meeting. Finally, we conducted structured interviews with representatives of defence companies and their suppliers, which played a key role in shaping the final draft. This final draft was then submitted for internal review by the Flemish Peace Institute and for external review by two experts.

In the second chapter of this report we explore the transition from voluntary due diligence standards to binding due diligence regulations, and also the challenges associated with implementing these standards and laws into practical due diligence measures. The third chapter provides an assessment of the current state of due diligence in the arms industry. The fourth chapter is the most critical, as it presents the key findings and insights derived from a study of due diligence practices in other industries, which offer valuable lessons and comparisons. Finally, the fifth chapter concludes the report with a summary of our findings and some final remarks.

1



Understanding due diligence

This chapter introduces the concept of due diligence as outlined in international soft-law frameworks. It then traces the evolution from soft law to binding legislation before concluding with a summarised overview of the key challenges associated with the practical implementation of due diligence processes.

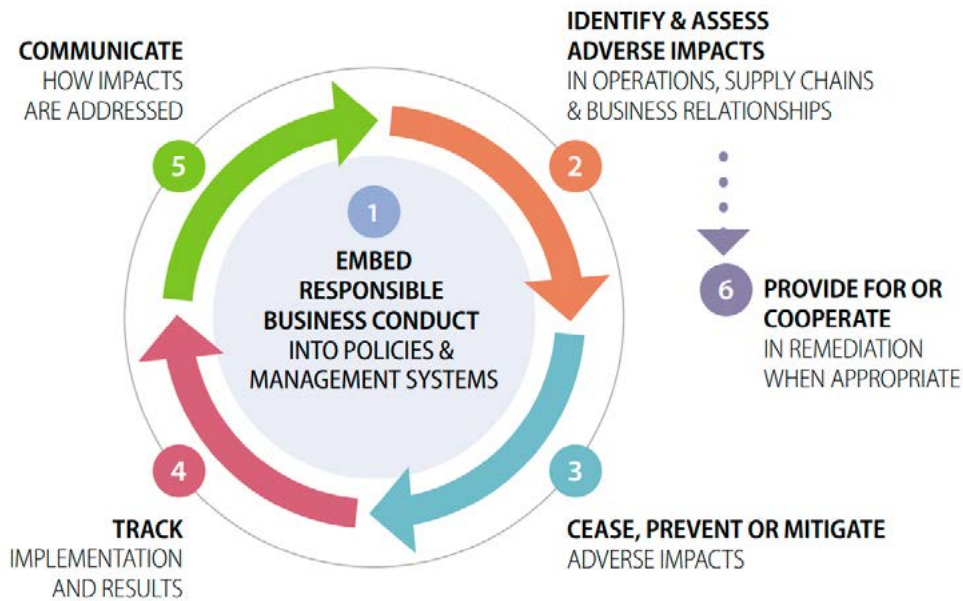
1.1 Due diligence standards

While the concept of due diligence has a much longer history – for instance, in the field of accounting and financial law – it is only with the adoption of the UNGPs in 2011 that it became associated with human rights. The UNGPs distinguish between three “pillars”. While the first (“The State duty to protect”) and third (“Access to effective remedy”) pillars deal primarily with the role of states, the second pillar (“II The corporate responsibility to respect”) outlines the expectations for companies. One of the key expectations is for companies to implement HRDD. That same year, the OECD included due diligence as a core concept in a revised version of its Guidelines for Multinational Enterprises.⁵ These guidelines were later accompanied by “Due Diligence Guidance for Responsible Business Conduct”.⁶

According to the OECD, due diligence involves a series of six parallel processes that are aimed at

- 1 embedding responsible business conduct into company policies and management systems;
- 2 identifying and assessing negative impacts;
- 3 taking action to prevent or reduce negative impacts;
- 4 tracking the results of these actions;
- 5 communicating about actions and results; and
- 6 ensuring adequate remediation for negative impacts that have occurred (see Figure 1).

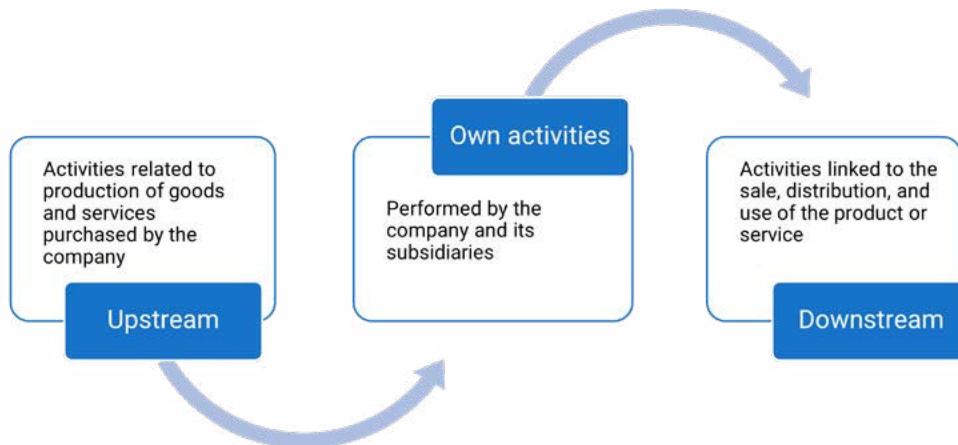
Figure 1: Due diligence according to the OECD



Source: OECD Due Diligence Guidance⁷

The UNGPs and OECD Guidelines contain two other important clarifications that are of immediate relevance to the defence industry. First, they emphasise that due diligence should be applied to a company’s entire value chain.⁸ In accordance with EU legislation, we understand a value chain as encompassing the entire lifecycle of products or services, which includes upstream activities in a company’s supply chain, the internal activities performed by a company and downstream activities related to the sale, distribution and use of products and services (see Figure 2). Second, both the UNGPs and the OECD Guidelines expect companies to carry out more extensive due diligence when their value chains extend into conflict-affected and high-risk areas (CAHRAs). Not only are these regions more susceptible to human rights violations, but the arms and military equipment produced by the defence industry often play a direct role in these violations.

Figure 2: Upstream, own activities, downstream



Source: own elaboration

1.2 Due diligence rules

Guidelines established by the OECD, which are non-mandatory at the outset, should be understood as political agreements between 38 member states which should require companies to comply with the standards contained in them. Always being one step ahead of regulation, they serve as the “source code” for legislation that requires companies to implement (aspects of) due diligence, a trend that has increased in recent years.⁹ While the hardening of due diligence rules can be observed in different jurisdictions (see, e.g., the Uyghur Forced Labor Prevention Act in the United States), it is particularly apparent inside the European Union. Below, we outline three key pieces of legislation and assess the ways in which they could affect the defence industry.

1.2.1 EU Taxonomy Regulation

The EU Taxonomy Regulation of 2020 provides a classification system for identifying environmentally sustainable activities. It is a key piece of the EU’s sustainable finance framework and it should help investors to make more sustainable investment decisions. While primarily focused on environmental considerations, the Taxonomy Regulation also has minimum social safeguards. Article 18(1) of the Taxonomy Regulation states that in order for an activity to qualify as sustainable, the company carrying out this activity must implement due diligence in accordance with the OECD Guidelines.

The Taxonomy Regulation has sparked intense debates about the stringency of the sustainability criteria and the types of activity that can be classified as sustainable. The defence industry, along with several other sectors (e.g., tobacco production and fossil fuels), has been completely excluded from the scope of sustainable financing. This could have important implications for the industry, because it could serve to strengthen existing exclusion policies exercised by banks and investors.¹⁰

1.2.2 EU Corporate Sustainability Reporting Directive (CSRD)

The Corporate Sustainability Reporting Directive (CSRD), which entered into force in January 2023, requires large companies (i.e., companies meeting two of the following criteria: turnover >€50 million, balance sheet total >€30 million, >250 employees) to include a detailed sustainability statement in their integrated annual report. This statement must expound on the “material” sustainability impacts, risks and opportunities throughout their entire value chain, including a company’s own operations and its upstream and downstream activities. In addition, it requires the company’s management practices to be disclosed, including due diligence processes, through which it seeks to manage these impacts, risks and opportunities.

For the defence industry, the CSRD has specific implications. Companies engaged in the production of or trade in controversial weapons – such as landmines, cluster munitions, chemical and biological weapons, and nuclear arms – are required to disclose both these activities and the revenue derived from them. The term “controversial weapons” refers to arms that are widely condemned for their indiscriminate and inhumane effects and which often violate international humanitarian laws and raise significant ethical concerns.¹¹ Beyond financial transparency, companies must also report on the broader impact of their activities, including how the sale and use of weapons might affect communities. They must also report on any measures they have taken to mitigate the negative impacts on these communities.

1.2.3 Corporate Sustainability Due Diligence Directive (CS3D)

In March 2024 EU negotiators reached a deal on the CS3D, which will require large companies (a phased approach, with the lowest threshold set at >1,000 employees and a turnover of >€450 million) to develop and implement due diligence policies that identify and mitigate adverse human rights impacts. Companies that cause adverse impacts on human rights or the environment and which have failed to carry out adequate due diligence can be held liable in a court of law.

While many observers were disappointed with the compromise deal, which was significantly watered down compared to earlier proposals, it is still a groundbreaking piece of legislation from a global perspective. Nonetheless, the CS3D deviates in a number of ways from international due diligence standards. Of particular relevance to this report is the fact that it excludes downstream impacts related to the sale and use of products and exempts products covered by national export controls (which include weapons, munitions, war materials and dual-use goods). With this exemption, the EU has seemingly confirmed the position that export controls suffice to assess the risks to human rights.¹²

However, it should be noted that the CS3D does cover the upstream part of defence companies’ value chains, which will oblige large defence companies to implement HRDD processes. It is also noteworthy that EU and US defence companies sourcing so-called conflict minerals are already required to implement due diligence processes in their upstream supply chains under the EU Conflict Minerals Regulation and the

US Dodd–Frank Act Section 1502, respectively (see the introduction to chapter 4). Consequently, many defence companies have already embarked on the due diligence journey, or are soon to be required to do so.

1.3 (Downstream) due diligence: challenges for corporate practice

While due diligence has been intensely debated in the academic literature, evidence of the way companies are putting due diligence into practice remains thin. Moreover, the available research mimics the regulatory bias towards upstream (supply chain) due diligence, to the detriment of downstream due diligence. Nevertheless, a number of challenges can be identified that are common to all companies attempting to implement HRDD. These challenges stem from the complexity of value chains and regulations and also from matters related to companies' resources and the leverage they exercise over business partners.

Challenge 1: Complex and opaque value chains

The global expansion of production and intense specialisation have led to the development of exceedingly complex global value chains (GVCs). A wide array of goods and services now emerge from an extensive network of interactions involving countless companies operating across the globe.¹³ Many GVCs are characterised by various layers of subcontracting, diverse regulatory environments and a multitude of labour practices. This complexity is compounded by the fact that companies operating across GVCs can have a strategic interest in maintaining opacity.¹⁴ The diamond industry, for instance, has sometimes been criticised for finding comfort in the opacity of complex supply chains to avoid associations with issues such as money laundering, corruption or adverse human rights impacts associated with diamond mining.¹⁵

While establishing visibility in the upstream segments of a value chain can be challenging, understanding the downstream segments of a value chain can be even trickier. Once a product or a service is sold in an open market, a company's ability to monitor that product or service may be diminished. And even if safeguards are in place to oversee the initial sale, if a company is not dealing with a controlled substance it often has little control over how clients decide to use a product, or over its resale, reuse or repurposing.¹⁶

In the specific case of the defence industry, arms deals often involve a high degree of confidentiality, frequently involve intermediaries, and they often take place in regions characterised by limited transparency. Pointing to national security justifications, many governments do not allow for arms revenues and expenditures to be examined. The level of parliamentary oversight of arms transfers, for example, varies widely between countries.¹⁷ This opacity can obscure the ultimate end-users and the specific purposes for which arms are intended, which in turn increases the risk of diversion to illicit markets or for unauthorised uses.¹⁸

Challenge 2: Regulatory complexities and a lack of clear guidance

Companies need to understand and navigate an exceedingly complex patchwork of regulations and norms across jurisdictions and sectors. While a growing number of standards and guidelines exist that can support companies in their due diligence processes, there is a lack of clear and actionable due diligence guidance for companies in the arms industry – although initial steps have been taken in this direction.¹⁹ Moreover, existing guidance focuses predominantly on supply chains, while overlooking downstream due diligence.

The arms industry is covered by a patchwork of treaties, national laws and regional agreements. Navigating this complex regulatory environment demands significant legal expertise and resources, rendering compliance a challenging undertaking.²⁰ Currently, some 35 regional and international arms control and disarmament agreements are in force worldwide.²¹ In addition, the need for arms transfer controls flows from general international law, specifically international humanitarian law and international human rights law. Incorporated into national legislation, these regional and international legal obligations give rise to government controls on the trade of both conventional arms and dual-use goods and technologies. In addition, informal multilateral forums seek to harmonise the control systems of participating states.

The ATT is the main binding multilateral instrument for the trade in conventional arms, while the Wassenaar Arrangement helps to shape the control systems related to such arms and dual-use goods and technologies – among other measures by establishing lists of items that should be subjected to government controls. State parties to the ATT must therefore organise export controls based on risk analyses that may or may not result in the granting of export licences. A key element in these assessments is determining the end-use and end-users of exported products. To this end, many countries require those companies applying for export licences to submit authorised end-use certificates.

In addition, companies must abide by multilateral arms embargoes of, for example, the UN and the EU, and specific trade sanctions such as those currently imposed on Russia and Belarus by the US, the EU and like-minded states.

At the regional level, the EU has the most elaborate legal framework to control transfers of arms and dual-use goods. For example, the EU Common Position 2008/944/CFSP regulates the control of exports of military technology and equipment, Directive 2009/43/EC lays down the conditions for intra-EU transfers of defence-related products and EU Regulation 2021/821 (EU Dual-Use Regulation) establishes a regime for the control of exports, brokering, technical assistance and the transit and transfer of dual-use items.

Varying from country to country, administrative procedures regarding export controls can pose a significant challenge, especially for SMEs that do not specialise in defence products. This applies not only to obligations vis-à-vis governments, but also to the

screening procedures of financial institutions whose regulatory compliance with respect to defence-related transactions is not satisfied by export licences alone.²²

Challenge 3: Capacity and leverage

Incorporating HRDD into company operations necessitates investments in expertise, management systems, stakeholder engagement, remediation and continuous improvement. These investments might pose barriers for companies, most notably for smaller companies with limited resources. Resources and capacity matter for another reason too: companies with significant resources and strong capacities are generally in a better position to exercise leverage over their business partners. While exercising leverage over upstream business partners (suppliers) is already difficult, companies may find their leverage over downstream business partners to be reduced even further.



2



(Downstream) due diligence in the defence industry

Governments' export licences do not protect defence companies adequately from multiple risks threatening their business interests. These risks occur in the financial, regulatory and legal spheres, and the trends of the past few years suggest that they are likely to increase.²³ Despite some signs of growing awareness of the need to assume responsibility for the human rights impact of its activities, including through exercising HRDD, the defence sector continues to lag behind most other industries.²⁴

This chapter delves into the financial, regulatory and legal incentives that motivate defence companies to implement HRDD. It highlights the increasing scrutiny by stakeholders, including the public and investors, together with the implications of legislative frameworks and legal accountability. In addition, the chapter examines the existing HRDD practices in the defence industry. Here, it emphasises the necessity for comprehensive due diligence that goes beyond mere compliance with government controls and explores proactive strategies to mitigate human rights risks associated with arms exports.

2.1 Financial, regulatory and legal incentives for exercising human rights due diligence

Defence companies face growing scrutiny by the public, media and civil society organisations, which can lead to reputational damage.²⁵ This trend is mirrored in increased shareholder activism and in ethical investors' excluding the defence industry from their portfolios.²⁶ Some investors have also mandated defence companies to report on their human rights impact and due diligence. Alternatively, investors are implementing HRDD programmes of their own.²⁷ Furthermore, banks and financial institutions are increasingly incorporating human rights considerations into their lending and investment decisions, urged as they have been to do so by legislators. This is the case with the EU Taxonomy Regulation (see chapter 2) and with civil society watchdogs reporting on the services they provide to companies in the defence sector.²⁸

In short, defence companies failing to conduct HRDD are increasingly facing barriers to entering certain markets or to accessing finance.

Human rights and related due diligence are also gaining ground in the regulatory domain. For example, human rights and international humanitarian law considerations have led governments, including the United Kingdom, Canada and Belgium,²⁹ to rethink some of their controversial arms export policies, with potentially important implications for the defence industry. Earlier, we have also seen that the concept of HRDD has become increasingly embedded in legislation that does not specifically target the defence industry but has direct implications for the industry, as in the case of the EU CSRD.

In addition, arms exporters face potential legal challenges, including criminal liability, for failing to comply with human rights and humanitarian law standards codified in domestic and international arms trade regulations. To the best of the authors' knowledge, there are no cases to date in which arms exporters have been convicted for licensed transactions unless there is evidence of misuse of licences or fraudulent application. However, legal experts caution that defence companies could face legal liability for inadequate due diligence, even if a particular export is covered by a valid licence, due to evolving interpretations of domestic and international regulations governing arms trade and human rights compliance.³⁰ Furthermore, European courts have annulled or suspended arms export licenses in cases brought by civil society groups, while similar cases are still pending in various countries in the EU and in the US.³¹ Finally, several arms companies and their officers have been accused of illegal arms sales, with recent convictions in Germany and cases pending in other countries.³²

Due diligence is a proactive approach to managing these risks because it allows companies to identify, assess and mitigate risks associated with their products and services. By conducting thorough HRDD, defence companies can defend themselves against legal risks proactively, improve their reputation and secure financial benefits. In other words, they should treat HRDD not merely as a regulatory requirement but as a strategic imperative they must embrace to navigate the exceedingly complex ethical, regulatory and commercial context of the modern defence sector.

The ethical implications of arms manufacturing and sales are profound and multifaceted. The defence industry operates in a landscape marked by significant moral complexities, where decisions about arms sales can affect human lives and regional stability directly. While the ethical considerations of exporting weapons to countries with a history of human rights violations may seem clear-cut, in reality there are many "grey zones".

These grey areas often involve sales to governments engaged in counter-terrorism operations or those asserting their right to defend national sovereignty, which can be framed as legitimate military actions. However, the distinction between legitimate and illegitimate use of force is often subjective and influenced by political, social and historical contexts. Questions arise about who determines the legitimacy of a conflict

or the acceptability of casualties. Is it solely the responsibility of the state receiving the arms or do manufacturers bear some moral obligation to scrutinise the potential end-use of their products?

This conundrum presents significant ethical challenges for defence companies, because they are required to navigate competing narratives about justice, sovereignty and human rights.³³ An ethical framework for assessing these risks must consider not only the immediate context of the sales but also the broader implications of the arms trade on global peace and security. The potential for complicity in human rights abuses creates a pressing need for defence companies to engage in deep reflection and discourse about their role in these complex issues. However, it is important to emphasise that the responsibility for making such assessments does certainly not fall solely on the companies; instead, it is a shared responsibility between states and companies, one requiring coordinated efforts to ensure ethical decision-making and accountability in the arms trade.

This understanding prompted the American Bar Association Center for Human Rights to issue an HRDD Guidance for the defence industry in 2022, drawing on the UNGPs, the OECD Guidelines for Multinational Enterprises and the OECD Due Diligence Guidance for Responsible Business Conduct as its primary sources.³⁴

2.2 Existing practices

A survey conducted in 2018 by Amnesty International, along with the Flemish Peace Institute's 2023 report on due diligence and corporate liability in the defence industry, demonstrated that major arms companies have policies that refer to human rights.³⁵ These policies are codified under titles such as "Human Rights Policy", "Code of Conduct (CoC)" and "Code of Ethics and Business Conduct". They focus primarily on upstream supply chain risks and issues related to the companies' own employees rather than on the risks associated with the sale and use of their products. When asked about specific arms sales and their human rights impacts, the surveyed companies often referred to legal compliance and government responsibilities.

A recent review has identified tentative language in the human rights policies of some major players regarding the potential adverse downstream impacts of their activities.³⁶ A small number of defence companies have begun to clarify aspects of their due diligence, such as excluding sales to undemocratic regimes, "sensitive countries" or customers with an unacceptable human rights risk profile. However, public availability of detailed information on due diligence standards and practices in the defence industry remains limited. Respondents from the defence industry confirm that these aspects of due diligence are common practice.³⁷

Moreover, these same respondents indicate that the most significant risks often lie with the brokers involved in arms transactions. Consequently, due diligence practices frequently focus on compliance checks on individuals and companies – particularly their beneficial owners – and sanctions lists. This approach, however, tends to

overlook the broader spectrum of human rights risks associated with the end-use of their products. Such risks can manifest in various forms, including the potential for weapons to be used in armed conflicts against civilian populations or in the repression of political dissent. Companies face complex ethical and political dilemmas in assessing these risks.

While established frameworks and red flags exist in other sectors, the lack of similar clear guidelines for arms exports presents challenges for these companies. One such framework, is the OECD Due Diligence Guidance for Responsible Supply Chains in the minerals industry, which outlines specific risk indicators such as sourcing from conflict-affected areas, the involvement of corrupt intermediaries and historical ties to human rights violations. This gap emphasises the necessity for a more nuanced approach to HRDD, one that enables defence companies to make informed decisions while recognising the inherent ethical dilemmas they encounter.

To assess human rights impacts, companies would need to engage with a range of indicators, including the political context of the purchasing country, the nature of the regime in power and prior instances of human rights violations associated with similar products. Red flags may include sales to countries with documented histories of using force against civilians or to regimes known for suppressing freedom of expression and assembly. Failure to deal with these considerations adequately can inadvertently lead arms companies to contribute to human rights abuses, which underscores the need for comprehensive due diligence that extends beyond mere compliance to include proactive measures aimed at preventing potential harm.

Despite these considerations, the global defence industry often operates under the assumption that government controls – typically encompassing export licensing procedures – satisfy the obligations for arms-exporting companies to conduct due diligence regarding human rights and international humanitarian law risks related to their products. Consequently, references to defence companies actively engaging in meaningful downstream HRDD are less prevalent.

The Norwegian defence contractor Kongsberg is considered an interesting example of good practice.³⁸ In its 2023 human rights report, the company describes its aim to take a 360-degree view of its entire value chain to understand the actual and potential risks through human rights impact assessments. The company acknowledges its responsibility to undertake such evaluations independently of government export controls. Kongsberg states further that its due diligence process aligns with the OECD Guidelines for Multinational Enterprises³⁹.

More indirect references to downstream HRDD in the global defence industry are about due diligence checklists for arms exporters issued by government authorities. Examples include a questionnaire from the Canadian Commercial Corporation,⁴⁰ which helps companies to secure contracts with foreign governments, and the Internal Compliance Program (ICP) of the Strategic Goods Control unit of the Flemish government, which provides HRDD guidance to arms and dual-use goods exporters. The Flemish ICP

emphasises that HRDD is an industry responsibility in interaction with but separate from government export controls.⁴¹ ICP guidance specifically in relation to dual-use goods has been issued within the framework of the Wassenaar Arrangement,⁴² the EU⁴³ and at the multilateral level.⁴⁴

Other governments have also recognised that the arms industry should not be exempt from its responsibility to respect human rights and to implement HRDD, as described in the UNGPs and the OECD Guidelines. This is highlighted, for instance, in a working paper submitted by Austria, Ireland and Mexico to the Conference of States Parties to the ATT in August 2023 (CSP9): the paper recommends keeping HRDD by defence companies on the CSP agenda for elaboration in the future.⁴⁵ In response, the conference adopted the decision to welcome the UNGPs and encourage “States Parties and other stakeholders to continue discussions on how the UNGP, Human Rights and international humanitarian law instruments apply in the context of the Arms Trade Treaty, as appropriate”.⁴⁶

These discussions open up new perspectives on integrating HRDD into the arms industry, but they also highlight the significant challenge of navigating this relatively new and complex theme. As stakeholders grapple with ways to implement these principles effectively, analysing and identifying practices and lessons learned from other sectors can provide valuable insights for advancing these discussions in the arms industry.

3



Lessons from other sectors

In this chapter, we examine the ways in which companies in three sectors other than the defence industry engage in due diligence. After introducing the rationale for including the technology, non-energy extractives and diamond industries, we discuss the emerging due diligence practices in these sectors in relation to each of the due diligence processes identified by the OECD (see Figure 1).

Technology industry. Technology companies have experienced growing pressures to deal with adverse human rights impacts in their value chains. In the upstream segment, the spotlight has long been on the human rights implications of resource extraction (contributions to armed conflict, but also forced labour and child labour in mines), although recent years have also seen growing scrutiny of the working conditions in technology manufacturing (e.g., exposure to toxic chemicals in electronics factories). Regarding downstream impacts, issues often relate to the (mis)use of digital technologies. For instance, while surveillance technology can support legitimate national security measures, it also poses risks to personal freedoms.⁴⁷ In addition, telecom providers or social media companies operating in countries with politically repressive regimes may inadvertently facilitate human rights abuses. This evolving risk landscape has led some technology firms to broaden their due diligence to include a focus on downstream impacts.

Non-energy extractives. Companies sourcing minerals risk contributing to human rights violations as the proceeds of mineral resources in some regions fuel conflicts. The pressure to create conflict-free supply chains of the minerals tin, tantalum, tungsten and gold (3TG) mounted when the UN Group of Experts on the Democratic Republic of Congo (DRC) released its final report in 2010, which illustrated in detail how both rebels and the national army were profiting from the mineral trade.⁴⁸ The UN Security Council subsequently expressed its support for the Group of Experts' due diligence guidelines.⁴⁹ Still in 2010, US president Barack Obama passed a provision on conflict minerals from the DRC and adjoining countries as part of (namely Section 1502) a Wall Street reform law referred to as the Dodd-Frank Act.⁵⁰ The Act imposes

due diligence obligations on businesses that trade on US Exchanges and are implicated in the supply chains of tin, tantalum, tungsten and gold (3TG), the four main metals extracted from eastern DRC ores.⁵¹ Subsequently, the OECD, in 2011, issued its Due Diligence Guidance for Responsible Supply Chains of Minerals from CAHRAs.⁵²

The OECD Guidance helps companies to implement responsible business conduct standards in their mineral supply chain and to prioritise the severe risks associated with mineral production and trade. In addition to serious human rights abuses, the Guidance responds to the risks associated with the involvement of non-state armed groups in mineral extraction and trade, dealings with public or private security forces, bribery and money laundering, and fiscal non-compliance. In 2017, the EU made the implementation of five steps (excluding step six, which is remediation) of the OECD Guidance a legal requirement for certain EU importers of 3TG through the Conflict Minerals Regulation.⁵³ Meanwhile, more than half of all companies in the global minerals industry are reported to demonstrate some level of uptake of the Guidance.⁵⁴ They have pooled resources in industry-wide initiatives, while a well-resourced and highly functional secretariat at the OECD ensures intensive follow-up.⁵⁵ It should be noted, however, that the industry still faces serious challenges with regard to value chain transparency. As a result, upstream due diligence in producing countries is poorly implemented.

Diamond industry. Around the turn of the millennium, amid negative media coverage on “conflict” or “blood diamonds” and UN Security Council embargoes on uncertified diamonds from war-torn Angola, Sierra Leone and Liberia, the diamond industry was challenged to develop a global control regime that would reassure consumers of the conflict-free nature of its image-sensitive product.⁵⁶ This regime was created through multi-stakeholder negotiations launched in 2000, which involved the industry, governments of diamond-trading countries and civil society. Named after the South African town where diamond mining major De Beers was founded in the 19th century, these negotiations became known as the Kimberley Process (KP).

The KP proved to be the first major push for transparent and ethical business practices in the global diamond sector and soon evolved into a multilateral trade regime. It does not have formal treaty status like, for instance, the ATT, but it does have legal force since participating countries must pass into law domestic legislation to establish a system of internal controls.⁵⁷ These controls underpin the certification of exported diamond parcels as “conflict-free”, with “conflict-free” narrowly defined as “not used by rebel movements to finance conflict”. Resting on the agreement of participants not to trade diamonds with non-participants and only to allow trade in certified stones, the KP functions through working groups – for example, those on monitoring and statistics – and bi-annual meetings, which results in consensus-based decisions being adopted formally by the KP Plenary.

The diamond industry offers a good example of the way state export controls and HRDD are mutually reinforcing. Diamond-mining majors and leading retailers introduced due diligence systems in the industry as a complement to the KP.⁵⁸ They realised that the

KP's scope was too narrow to meet consumer expectations and therefore they created their own ethical sourcing protocols, which cover human rights and environmental standards.⁵⁹ Those company-specific self-regulatory due diligence systems are complemented by the Responsible Jewellery Council's certification mechanism, an industry initiative catering to the entire supply chain.⁶⁰ This means that a large part of the diamond pipeline, from mine to retail, is covered by auditable responsible business conduct schemes.

However, challenges remain throughout the global diamond value chain, which is characterised by the contrast between its fragmented midstream segment, with high levels of consolidation at both ends of the diamond pipeline, where five mining majors account for about 70% of global production, and large retail groups account for more than one-third of all sales to consumers.⁶¹ The opaque midstream of thousands of traders, cutting and polishing outfits, and manufacturers across the globe needs more transparency as it remains vulnerable to illicit diamond flows and money laundering.⁶² Finally, the sector as a whole would benefit from the more substantive and credible auditing of its due diligence systems.⁶³

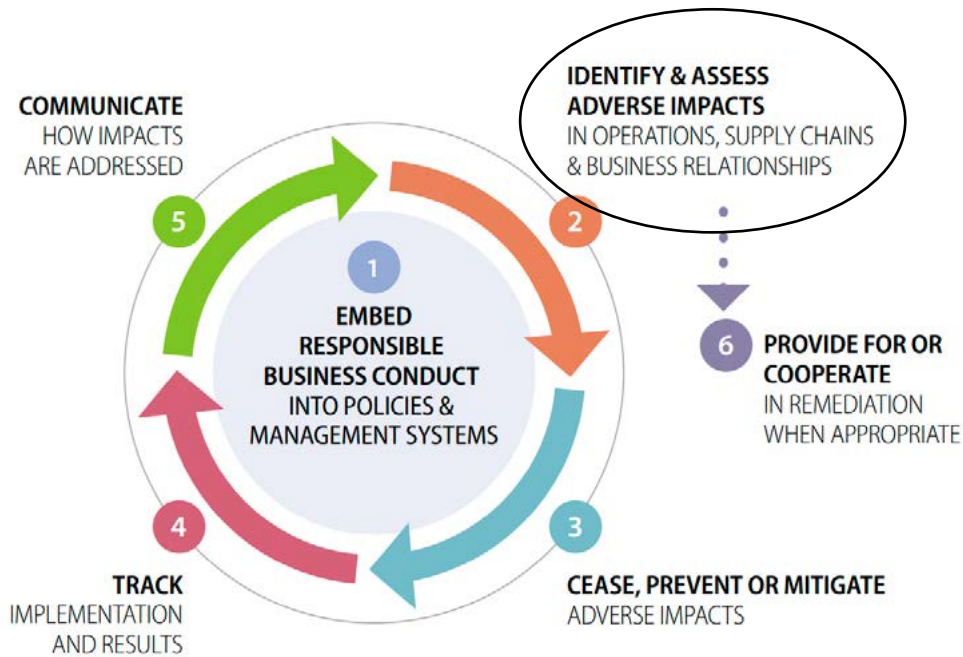
In the following sections, we discuss the key lessons that can be gleaned from these other sectors, and we assess their transferability to the arms industry.

3.1 Identify and assess impacts

While it is sometimes assumed that a full and detailed understanding of a company's entire value chain (including the names and addresses of all the actors involved in it) is a prerequisite for identifying (potential) adverse impacts, the OECD emphasises that companies should start with a "broad scoping exercise" to create a "high-level picture" of their value chain and to identify general risk areas.⁶⁴

Across all three sectors, risk assessments in the context of due diligence processes have mostly focused on upstream (supply chain) risks. However, a small number of companies in the technology industry have adopted a more holistic value chain approach. In the coming years, this trend will probably be reinforced by new reporting rules (notably the European CSRD) which will require companies to identify and disclose sustainability impacts across their entire value chain and to report on how they are managing these impacts.

Figure 3: Due diligence according to the OECD – step 2 'identify and assess impacts'



ZOOMING IN: Ericsson’s 5G impact assessment⁶⁵

In March 2021, Ericsson initiated a pioneering drive to evaluate the human rights implications of the roll-out of 5G technology. The company’s comprehensive assessment was developed in collaboration with Shift, a leading human rights centre of expertise. It involved extensive research and consultations with both internal and external stakeholders. Several methodological challenges had to be overcome, such as the broad scope of 5G’s applications and the multitude of potentially affected stakeholders, in addition to the highly dynamic nature of emerging technologies. This approach led to a wide range of human rights impact areas being identified in relation to Ericsson’s downstream value chain. Prominent areas include the job market impacts of automation and AI, the health and safety risks of 5G infrastructure deployment, the privacy and data security risks, ethical concerns about surveillance capabilities and network shutdowns, and ensuring equitable access to 5G technology to avoid exacerbating societal inequalities.

Once a more high-level picture of (risks across) a value chain has been obtained, companies should proceed towards a more granular risk assessment of specific activities and business relationships. Here, companies will typically consider a number of parameters:

- 1 Location risks.** Some countries and regions are considered to be more at risk than others. To assess location risks, companies often rely on databases and indices such as the World Bank’s Worldwide Governance Indicators [Worldwide Governance Indicators](https://www.worldbank.org/en/publication/worldwide-governance-indicators)^a for governance quality, the [ITUC global rights index](https://www.etuc.org/sites/default/files/press-release/file/2023-06/ITUC-Global-Rights-Index-2023.pdf)^b for labour rights

a <https://www.worldbank.org/en/publication/worldwide-governance-indicators>

b <https://www.etuc.org/sites/default/files/press-release/file/2023-06/ITUC-Global-Rights-Index-2023.pdf>

or the list [conflict-affected and high-risk areas](#)^a, commissioned by the European Commission.

- 2 Risk management practices of business partners.** To assess the extent to which business partners respect human rights, companies can carry out their own assessments based on desk research or supplier questionnaires, or they can rely on the services of specialised companies (see section 3.4.2). The screening of business partners should focus not only on whether the business partner has previously been linked to adverse human rights impacts, but also on whether the business partner has adequate due diligence systems in place.
- 3 Risks tied to the nature of a product or production process.** Some activities and production processes are more closely associated with human rights risks. Examples include activities that rely on a large and unskilled workforce (e.g. apparel production); activities that involve the extraction of high-value “point resources” such as gold and coltan; and activities that involve vulnerable (migrant) workers (e.g., horticulture).

Risk assessments of upstream business partners are becoming increasingly common, and an entire industry has emerged to support companies with such assessments. Meanwhile, assessments of downstream business partners in the context of due diligence remain scarce. BSR, a sustainable business network and consultancy firm, has developed a guide which outlines some of the questions that companies need to ask when assessing risks in their downstream value chain.⁶⁶ HP Enterprise and Ericsson provide good examples of companies that are undertaking efforts to integrate human rights into their downstream business relationships (and more specifically into sales).

ZOOMING IN: Integrating due diligence into sales – the experience of the tech sector

Ericsson has integrated due diligence into its sales process through its Sensitive Business Framework. All sales opportunities are reviewed to flag high risks across four checkpoints: product risks (what technology is being sold); use risks (what is the product's intended use); client risks (who is the potential buyer), and country risks (where will the technology be used). Any sales opportunities that reach a certain threshold of combined risk across these checkpoints must be screened by the Sensitive Business Core Team. The decision can be to approve a sales engagement with or without conditions or to reject it outright. For instance, for products with heightened risks, greater restrictions can be placed on selling into high-risk regions.⁶⁷

HP Enterprise (HPE), a global technology company that provides a wide range of enterprise-level solutions, has similarly integrated human rights considerations into its sales processes. Specifically, HPE screens sales opportunities by assessing the degree, nature and probability of risk, based on KYC principles (notably existing human rights allegations), geography, product and intended use (including heightened attention for surveillance-enabling technologies). Where this screening reveals obvious risks, it can lead to the inclusion of sales conditions, or even to the outright rejection of sales opportunities.⁶⁸

a <https://www.cahaslist.net/cahras>

Other interesting practices can be observed when we expand our scope beyond human rights. Companies in different sectors are expected to put in place KYC procedures to assess risks related to financial crime. According to BSR, KYC procedures could be an interesting starting point for integrating human rights considerations.⁶⁹ In the financial sector, for instance, there are growing calls for banks to integrate Environmental, Social and Governance (ESG) risks into KYC processes.⁷⁰ Of the three sectors included in this report, the diamond industry is undoubtedly the one where KYC processes are most established.

ZOOMING IN: KYC and human rights in the diamond industry – a work in progress

An example of good practice in KYC risk screening can be found in the diamond trading hub Antwerp.⁷¹ The industry's representative body, the Antwerp World Diamond Centre (AWDC), provides all registered diamond dealers with a free tool to identify any risks related to their customers and business relationships. This helps its members to comply with anti-money-laundering legislation. The tool is the Bureau van Dijk⁷² database, which is continuously updated by business intelligence providers across the globe and provides ratings based on risk indicators. The database includes identifying information on directors and beneficial owners. It checks whether they or their company appear on sanctions or enforcement lists or in adverse media, whether they are politically exposed persons, and whether the company is based in high-risk countries.

In 2023, and together with one of the authors of this report, AWDC screened the market to see if there were any KYC solutions that integrated considerations related to human rights and environmental impacts. The key findings that emerged from this screening were: (1) that mainstream KYC solutions such as Bureau van Dijk do not yet offer comprehensive risk solutions, and (2) that the existing tools for undertaking sustainability screenings of business partners were primarily focused on upstream suppliers and are not yet ready to accommodate the specific realities of the diamond industry.

Many companies will face a wide range of actual and potential adverse impacts. According to the OECD, when it is not possible to respond to all these impacts simultaneously, companies should prioritise them based on their severity and, in the case of potential impacts, their likelihood.⁷³ Severity is assessed using three key parameters:

- 1 Scale:** Scale refers to the gravity of a (potential) impact. For example, the loss of life is considered far more severe than instances of petty corruption. This parameter helps companies to gauge the seriousness of an impact by considering the magnitude of the harm caused.
- 2 Scope:** Scope refers to the reach or extent of a (potential) adverse impact. For instance, large-scale violations of humanitarian law are considered to be more severe than a single incident, such as one murder committed with an unregistered firearm. This parameter assesses how widespread the impact is and how many people or communities are affected by it.
- 3 (Ir)Remediability:** Remediability refers to the ease with which a situation can be reversed to its state before the adverse impact occurred. For instance, environmental pollution from an oil spill is often seen as less remediable than damage to a building, which can be repaired relatively quickly and easily. This parameter helps companies

to understand the long-term implications of a particular impact and the challenges associated with restoring the original conditions.

Applying these parameters in practice is not an easy exercise, as it involves navigating complex ethical considerations and measurement challenges. Companies must weigh the moral implications of their decisions, often dealing with subjective judgments about the relative severity of different impacts. In addition, accurately measuring the scope and scale of potential impacts can be difficult, especially in situations where data are limited or where the impacts are not immediately apparent.

Identifying impacts: relevant lessons for the defence industry

In the sectors we examined for this study, the focus of HRDD has so far been mainly on upstream supply chains, which many defence companies are also (somewhat) familiar with due to their experiences with the implementation of conflict mineral regulations in the US and the EU. However, a number of frontrunner companies, such as Swedish tech firm Ericsson, are already quite advanced in developing practices that include the downstream part of their value chain in the risk identification and assessment phase. Consultancies such as BSR offer practical tools for this, while the American Bar Association Center for Human Rights has provided guidance to the defence industry, including recommendations for every step of downstream HRDD.

In the global defence industry, some major players have included language in their human rights policies that hesitantly acknowledges the potential adverse impacts associated with the sale and use of their products. It is to be expected that new reporting rules, such as the EU CSRD, will require defence companies to articulate their downstream risks more explicitly.

The technology and communications sector, in particular, offers them examples of how to identify and assess those risks. Defence companies can also use the tools developed in other sectors to assess risk parameters such as geographic location and risk management practices of business partners, as part of their customer vetting procedures. Many of them reportedly use the Orbis (formerly Bureau Van Dijk) database to screen customers, a tool that is also widely used in the diamond industry. Moody's Analytics, the parent company of Orbis, is said to be in the process of developing a module that will allow users to check the ESG performance of their clients for the purposes of compliance with the EU CSRD.

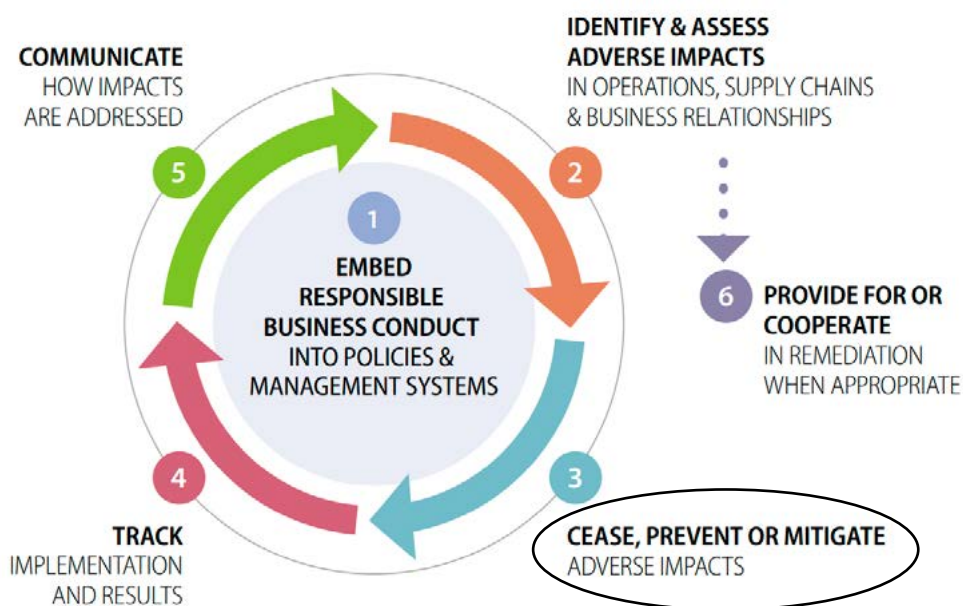
3.2 Taking action to prevent or minimise impacts

Having identified and prioritised (potential) adverse impacts, companies are then expected to develop and implement mitigative actions. The type of action a company is expected to take varies based on its involvement in an impact. When companies directly cause impacts themselves, they should take immediate action to end and remediate the impact. For this report, we are mainly interested in instances where a company is (potentially) linked to impacts through a third party that is misusing its products. In this kind of situation, due diligence standards expect companies to exercise leverage to ensure that the third party takes mitigative measures to prevent, mitigate or remediate negative impacts.⁷⁴ Leverage can be understood as the ability of a company to influence changes in the operations or practices of a third party. It can be derived from different sources and exercised in multiple ways.⁷⁵

3.2.1 Contractual leverage

The primary way in which companies traditionally seek to exercise leverage over business partners is through contracts. In the case of upstream risks, a growing number of companies are adopting a supplier CoC that contains expectations in domains such as ethical business conduct, environmental responsibility and human rights. Under the new European CS3D, companies will be required to have a CoC in place and to seek contractual assurances from business partners that they will adhere to it.

Figure 4: Due diligence according to the OECD – step 3 ‘cease, prevent or mitigate impacts’.



While a CoC can be an important tool with which to communicate a company's values and commitments to business partners, its effectiveness hinges on (1) the implementation of robust verification mechanisms and (2) appropriate responses to instances of non-compliance.⁷⁶ Ideally, therefore, the CoC should contain a description of the way compliance with it will be monitored, and also of the consequences of non-compliance – which could include the possibility of terminating the relationship. In the context of downstream due diligence, contractual leverage would imply that companies integrate human rights safeguards into sales contracts, licensing and service agreements, warranty documents, etc. Such safeguards and controls could include stipulations such as defining a product's intended use, restrictions on the resale of the product or requiring clients to impose sales restrictions on their clients.⁷⁷

ZOOMING IN: HPE enterprise partner code of conduct⁷⁸

Many large tech firms rely on partners for the sale and distribution of their products. In most cases, (potential) adverse impacts are not located at the level of these partners but further downstream. For this reason, in addition to having adopted a supplier CoC, HPE Enterprise has also adopted a "Partner CoC" in which it outlines its expectations of its partners (which include distributors, resellers and agents). Among other things, partners are expected to take "reasonable steps to ensure that customers use HPE products responsibly and avoid sales to those who intend to use HPE products in a manner that might infringe on the human rights of any individual", and to establish "procedures for appropriate risk-based due diligence on third parties".

3.2.2 Disengagement

When assessments reveal human rights concerns in relation to new business partners or opportunities, deciding against partnership may be wise. The decision-making process is often more complicated for existing business relationships, though: the strategic or commercial significance of the relationship may make it impractical to end it. Moreover, as demonstrated by conflict minerals legislation, abruptly severing business ties can inadvertently harm human rights. This insight supports the principle found in due diligence standards and in European legislation that disengagement can be only a very last resort, when all other efforts to exercise leverage have failed.

ZOOMING IN: Disengagement- the experience of conflict minerals

Section 1502 of the Dodd-Frank Act encourages increased scrutiny of conflict financing through the proceeds of the mineral trade in the African Great Lakes region. Consequently, most international mineral traders stopped sourcing minerals from the DRC altogether, a phenomenon referred to in the region as a "de facto embargo". As a result, an estimated 2 million people experienced dire socio-economic consequences, including reduced income, increased theft, a sharp decline in all local trade, an increase in school dropouts, etc.⁷⁹ Another consequence was that the Congolese army and police took advantage of the situation to intensify their illegal mining activities.

However, when business partners consistently ignore efforts to deal with and mitigate risks, disengagement can become unavoidable. Moreover, the severity of some (potential) human rights impacts may warrant immediate disengagement.⁸⁰ Finally, a credible threat of disengagement can itself act as a lever to influence partners towards

positive change. This is also why the option to terminate a partnership is often included in a supplier CoC.

The available evidence on disengagement mostly relates to upstream business partners. For instance, Nestlé has previously severed ties with Indonesian palm oil producers over concerns related to land-grabbing and human rights abuses.⁸¹ And tech giant Apple has repeatedly severed ties with suppliers over allegations of forced labour and child labour.⁸² Evidence on disengagement from downstream business relationships due to human rights considerations is rare, though. Such disengagement could take the form of the cessation, suspension or refusal of services or sales if misuse is suspected.⁸³ A number of cases exist in the financial sector. For instance, in 2021, several major European lenders decided not to finance the construction of the Total-SE-sponsored East African Crude Oil Pipeline due to human rights and environmental concerns.⁸⁴

ZOOMING IN: Ending an existing business relationship—the case of Newtec

In November 2018, Newtec, a Belgian satellite company, faced mounting pressure after being included in a “dirty list” compiled by the Burma Campaign UK, which identifies companies with ties to the Myanmar military. This scrutiny stemmed from Newtec’s business dealings with Mytel, a telecommunications operator in Myanmar partially owned by the military, amid allegations of human rights abuses, particularly against the Rohingya minority. Headquartered in Sint-Niklaas, Belgium, Newtec specialises in satellite communication technology, striving to bridge connectivity gaps in underserved regions globally. With growing concerns over its association with Mytel and potential complicity in human rights violations, Newtec announced its decision to sever ties with Mytel in August 2019.⁸⁵ This case underscores the necessity of effective due diligence, recognising that in certain instances terminating existing business relationships becomes imperative, especially when the business partner is directly involved in human rights abuses and shows no indication of reforming its practices.

3.2.3 Working with business partners

The standard practice for upstream due diligence is for companies to adopt a supplier CoC and then to monitor compliance with this CoC through audits (see section 3.4). When instances of non-compliance are identified, business partners will be expected to implement “corrective actions”. But there is growing consensus that this top-down, “policing style” approach to due diligence has clear limitations.⁸⁶ For instance, it could end up encouraging superficial compliance or lead to the root causes of non-compliance being overlooked, such as unfair pricing or a lack of capacity on the part of suppliers. Slowly but surely, a new consensus is emerging about the need for engagement with and support for business partners.

At a minimum, companies should engage in regular and open conversations with business partners about the expectations, challenges and practicalities of implementing due diligence. In this way, they are able to obtain insights into the operational realities of business partners, enabling more tailored support and more effective interventions. Companies can also incentivise responsible business conduct through recognition

programmes or preferential business terms. Finally, companies could educate and train business partners about the importance of paying attention to human rights.

*ZOOMING IN: Apple's approach to supplier engagement*⁸⁷

In recent years, Apple has come under scrutiny due to allegations of human rights violations within its supply chain. Reports have emerged about breaches of labour law at iPhone manufacturing facilities, where workers were found to be subjected to working excessive overtime and being penalised for failing to meet targets.⁸⁸ To redress these concerns, Apple has intensified its due diligence processes. The company has implemented a detailed Supplier CoC and engages in thorough evaluations to ensure adherence throughout its worldwide supply chains. This includes conducting independent audits. To enhance the understanding and enforcement of its CoC further, Apple has initiated various educational programmes aimed at providing suppliers and their employees with opportunities for education and skills development. In 2022, Apple launched a \$50 million Supplier Employee Development Fund to strengthen these educational efforts. Moreover, Apple partners with global organisations such as the International Organization for Migration and the International Labour Organization. These collaborations aim to improve the efficiency of its training initiatives and encourage the industry-wide adoption of best practices.

While examples of engagement with downstream business partners are harder to find, many companies already facilitate training with sales partners on topics such as business ethics and compliance. Basic training in human rights or responsible product use could be integrated into these training sessions – for example, by including practical guidance on how to identify clients or sales with high human rights risks.⁸⁹

3.2.4 Working with external experts

To adapt to growing human rights expectations, many companies enlist the support of “external experts” who can provide vital knowledge or they facilitate conversations with key stakeholders.⁹⁰ Auditors constitute a first important group of experts. They can verify not only adherence to human rights standards (which include but are not limited to CoCs), but also human rights reporting. Yet, unlike the established domain of financial auditing, sustainability auditing is in its infancy and encounters obstacles such as the lack of uniform practices.⁹¹ In addition, the mostly qualitative nature of human rights information underscores the critical role of auditors' expertise and judgement.⁹² Scrutiny of auditors and their methodologies is intensifying, a topic we delve into more thoroughly in section 3.4.

A second group of external experts, which overlap with auditors, are consultants. The field of sustainability consulting is diverse, ranging from large firms such as KPMG and Ernst & Young (EY) to smaller boutique consultancies focusing on specialised services such as due diligence. Consultants can help companies link complex standards and regulations to business practice. However, the “big four” in particular have also faced criticism for endorsing compliance-focused strategies that may place regulatory compliance above dealing with the root causes of adverse human rights impacts.⁹³

3.2.5 Collective action through industry and multi-stakeholder initiatives

The leverage that individual companies wield over business partners is often limited. In recent years, there has been a proliferation of joint initiatives to respond to sustainability challenges in global supply chains. Many of these initiatives revolve around a voluntary sustainability standard (call it a collectivised CoC) that is enforced through audits and which may or may not be coupled to a certification scheme. A key distinction can be made between industry initiatives and MSIs: whereas the former are primarily composed of and controlled by business, the latter also involve (to varying degrees) civil society, government and other stakeholders. To illustrate the different approaches to addressing sustainability challenges in global supply chains, we will examine three prominent initiatives, each representing distinct models of collaboration and governance.

The **Responsible Business Alliance (RBA)** (<https://www.responsiblebusiness.org/>) is an industry initiative established in 2004 as the Electronic Industry Citizenship Coalition. Its founding motive was to ensure that the manufacture of products does not contribute to human rights abuses or environmental destruction. The RBA is structured around a secretariat that coordinates activities across different working groups, focusing on issues such as labour, health and safety, and environmental compliance. Its approach revolves around a joint RBA CoC that is enforced through the Validated Audit Process, which is designed to monitor compliance with the RBA CoC on the part of members and their suppliers. The collaborative aspect of the RBA's approach is most evident in the fact that audit findings and best practices are shared between members. Members are also encouraged to learn from one another in a wide variety of events and training sessions. Finally, the RBA puts various tools and resources at its members' disposal to support their due diligence efforts.

The **Responsible Jewellery Council (RJC)** is a London-based not-for-profit standards-setting and certification organisation with more than 1,800 members across the entire jewellery supply chain (mine to retail).⁹⁴ It was founded in 2005 by several industry associations and major corporations to promote consumer confidence by responding to ethical, social and environmental issues at every point in the supply chain on a global scale. The RJC strongly emphasises due diligence and has developed several tools for its members to implement it. For example, the RJC offers separate toolkits for HRDD and responsible sourcing of diamonds from CAHRAs. Members currently also receive guidance to support them in the implementation of the G7 Russian diamond import restrictions.⁹⁵ This comes after the organisation was plunged into turmoil following Russia's invasion of Ukraine, which triggered measures against one of its most prominent members, diamond mining giant ALROSA. Majority-owned by Russian government shareholders, ALROSA decided to end its RJC membership in April 2022, leaving its vice-chair on the board vacant.⁹⁶

An interesting recent development in the minerals sector is the **Initiative for Responsible Mining Assurance (IRMA)**. IRMA markets itself as “the world's most

rigorous mining standard” and is a consensus-led multi-stakeholder organisation in which the private sector, civil society and mining communities participate.⁹⁷ This inclusive governance model provides guarantees of audit independence, whereas IRMA also maintains an exceptionally high level of transparency regarding the publication of audit results.⁹⁸ IRMA therefore accompanies industrial mining operations in a trajectory of performance improvement on its 40 “critical requirements”. These requirements include business integrity, legacy planning, and social and environmental responsibility. Based on these and other experiences⁹⁹ with collective action in the domain of due diligence, a number of important observations emerge.

Experience to date allows us to make a number of observations about the role and functioning of MSIs and industry initiatives.¹⁰⁰

- 1 MSIs, owing to their more inclusive nature, can enhance the legitimacy and credibility of due diligence processes and this can lead to more comprehensive solutions that reflect the interests of diverse stakeholders. Industry initiatives, while by definition less inclusive, could capitalise on deep industry knowledge and tend to enjoy broader support from within the business community. This insider perspective allows for the creation of solutions that are more attuned to the practical realities of the industry, fostering quicker adoption and implementation.
- 2 Ideally, both MSIs and industry initiatives should be built on a comprehensive standard that aligns with established due diligence standards, such as those from the OECD or the UN. By adhering to a consistent standard, these initiatives can ensure uniform practices across the industry, reducing discrepancies and ensuring that companies are moving towards compliance with emerging regulatory requirements. This alignment not only helps companies to meet their legal obligations but also strengthens the overall effectiveness and integrity of initiatives.
- 3 For joint initiatives in responsible business conduct to function smoothly, robust support structures are essential. This includes having a dedicated secretariat to manage day-to-day operations, coordinate activities and ensure effective communication among stakeholders.
- 4 To secure commitment from the business community, the benefits of participating in MSIs or industry initiatives must be clear and tangible. As legislative pressures and public expectations of responsible business conduct continue to grow, the advantages of being part of these initiatives – such as reduced regulatory risk, enhanced reputation and improved stakeholder relations – will become increasingly apparent.
- 5 Independent monitoring is crucial to maintaining the credibility of any collaborative initiative and the standards it upholds. Regular transparent assessments by third-party monitors help to ensure that the participants are adhering to agreed-upon standards and that the initiative is making real progress. This external oversight is key to building and maintaining trust among stakeholders, because it provides the assurance that the initiative’s commitments are being met.

Note that industry initiatives are not alien to the defence industry. For example, umbrella organisations from the aerospace and defence sectors in the US and the EU have established the standards-setting International Forum on Business Ethical

Conduct (IFBEC), but this forum deals mainly with corruption and bribery, not with human rights.¹⁰¹ Similarly, the Defense Industry Initiative (DII) on Business Ethics and Conduct lays out principles for the business dealings of its members with the (US) government.¹⁰²

Mitigating impacts: relevant lessons for the defence industry

As in other industries, corporate leverage in the defence industry depends on factors such as the size of a company and its position in the value chain. At the top of the pyramid comprising many thousands of SMEs and several tiers of large contractors are lead integrators of weapons systems, or manufacturers of small arms and light weapons (whose value chains are less complex). The difference from other sectors is the central role of governments in driving demand, as customers (through defence procurement) and promoters carrying out the governments' foreign and defence policies, but also as regulators. In Western countries, regulations include human rights and international humanitarian law provisions that should be taken into account in governments' risk assessments during export controls.

In practice, however, the application of human rights stipulations in the law is a matter of interpretation, subject to the discretion of each government and characterised by a lack of transparency, including that vis-à-vis the defence companies concerned. Thus, when applying lessons from other sectors to the defence industry and assessing corporate leverage in it, one must keep the parameter of political power firmly in mind. For instance, providing weapons to controversial end-users such as the Israeli or Saudi Arabian militaries may contradict the values a defence contractor (c)laims to uphold. However, clashing with a partisan government customer may be seen as a greater business risk compared to any legal, investor or reputational risk involved in such transactions.

This said, the following takeaways can prove to be of value as defence companies embark on the journey towards downstream HRDD in their industry.

Contractual leverage

In the context of HRDD, contractual leverage implies that companies integrate human rights safeguards into sales contracts, licence and service agreements, warranty documents, etc. Such safeguards and controls could include stipulations such as defining a product's intended use, restrictions on the resale of the product or requiring clients to impose sales restrictions on their clients. In the arms industry, such stipulations

are, or should be, contained in the end-user certificates submitted to the export-controlling government authorities. However, government monitoring, especially that beyond the first sales tier, can be limited. To extend such monitoring to the later stages of an arms transfer, some exporting states have introduced post-shipment controls – for example, those taking the form of on-site post-delivery verification inspections.

Companies in the tech industry, such as HPE and Ericsson, have integrated human rights policies into their sales processes, providing instructive examples of how to operationalise downstream due diligence principles.

Disengagement

Disengagement by companies from downstream business relationships due to human rights considerations is rare. In the defence industry, reputational and financial risks surrounding contract termination are compounded by a lack of clarity regarding the boundaries between corporate and government responsibility. However, instances such as the Belgian tech company Newtec cutting ties with the Myanmar military junta amid allegations by civil society watchdogs highlight the importance of thorough due diligence.

Working with business partners

In the sectors examined in this study, quite a number of companies facilitate training sessions with sales partners on topics such as business ethics and compliance. Basic training in human rights or responsible product use could be integrated into these training sessions – for example, by including practical guidance on how to identify clients or sales with high human rights risks. Interviewees confirmed that similar practices exist in the defence industry. For example, one of the experts in our panel discussion indicated that some defence companies oblige customers to provide training to armed forces on how to make responsible use of their products.

Working with external experts

The use of auditors and consultants in HRDD is not without its problems. Owing to the primarily qualitative nature of human rights auditing, the experience of auditors is critical, whereas the field is still in its infancy. The consulting practices of the “big four”, in turn, have been criticised for their one-sided focus on compliance. There are also smaller “boutique” human rights consultancies. The Norwegian defence contractor, Kongsberg, for example, hired a specialised firm to help it define the outlines of its HRDD policy and may continue the collaboration in the future.

Industry and multi-stakeholder initiatives

In practice, defence contractors typically operate under the assumption that governments, through their export controls, bear full responsibility for the human rights impacts of defence-related equipment. However, interviewees from the defence industry point out that the demarcation between the responsibilities of governments and those of (suppliers to) defence companies is not sufficiently clear.

There is a risk that defence companies remain stuck in a passive role, waiting for governments to assign them clear responsibilities through legislation, which then adds downstream HRDD to their "burden of compliance". This may or may not happen in the foreseeable future. Meanwhile, the defence industry could seek proactively to form a coalition of corporate actors who are willing to enter the conversation.

On this point, our panelists and interviewees suggested several scenarios. For example, manufacturers of a certain type of high-impact military product, such as small arms and light weapons, could form a pilot coalition to discuss downstream HRDD. Also, industry associations such as the Aerospace, Security and Defense Industries (ASD) in the EU or the Aerospace Industries Association (AIA) in the US, could take the lead in creating a "coalition of the willing", building on the work already done on corruption and ethics in public procurement (IFBEC; DII). This would expand on the already existing practice of groups of trusted companies that benchmark one another's due diligence practices while collaborating on projects under the leadership of large system integrators.

From the above it is clear that government actors should be part of the conversation from the outset. Some governments have already demonstrated their commitment to assigning HRDD responsibilities to companies under their jurisdiction (see section 2.2) and could therefore prove to be valuable partners.

A key lesson from the sectors examined in this study is that (cross-)sectoral initiatives successfully create economies of scale and facilitate mutual learning, whereas multi-stakeholder models add legitimacy and credibility to such initiatives by engaging governments and civil society organisations in seeking to redress human rights issues, as has been amply demonstrated in the diamond and conflict minerals sectors.

Specific points to consider are the need to tailor OECD Guidelines to the defence industry; the need for a secretariat to manage day-to-day operations, and the importance of the credible, impartial and transparent monitoring of HRDD measures.

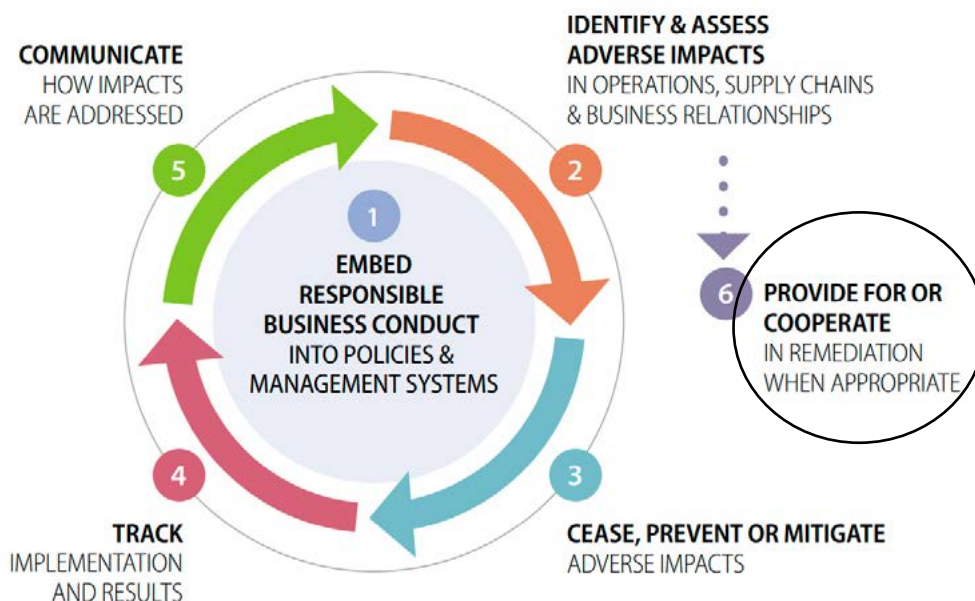
Remediation

The issue of remediation is, unsurprisingly, highly controversial in the defence industry and brings to the forefront the question of government versus corporate responsibility. It is, however, beyond the remit of this report to engage in such normative discussions – suffice to say that this issue needs to be dealt with in future HRDD conversations between the stakeholders concerned. Meanwhile, it may prove rewarding to consider the remediation initiatives in place in the tech and minerals sectors, such as the Fair Cobalt Alliance (FCA), which deals with the issue of child labour in Congolese cobalt mines.

3.3 When things go wrong: remediation

Remediation involves efforts to restore affected person(s) – or nature – to the situation they would be in if an adverse impact had not occurred.¹⁰³ Remediation could include financial compensation, restitution (e.g., of lands), rehabilitation (in jobs) or adopting measures to prevent future impacts. When a company is directly causing or contributing to adverse human rights impacts, it has a clear responsibility to provide for – or contribute to – remediation. For this purpose, companies are expected to establish “operational-level grievance mechanisms”, such as in-house or third-party complaints mechanisms.

Figure 5: Due diligence according to the OECD – step 6 ‘remediation’.



For the purposes of this report, however, we are mainly interested in instances where companies are linked to impacts through their business partners. According to the UN Guiding Principles, while a company that finds itself in such a situation has no strict obligation to provide for remediation,¹⁰⁴ the expectation is nonetheless that efforts are made to exercise leverage in order to ensure that the third party takes steps towards effective remediation. At a minimum, companies are expected to cooperate in good faith with judicial or non-judicial grievance mechanisms.

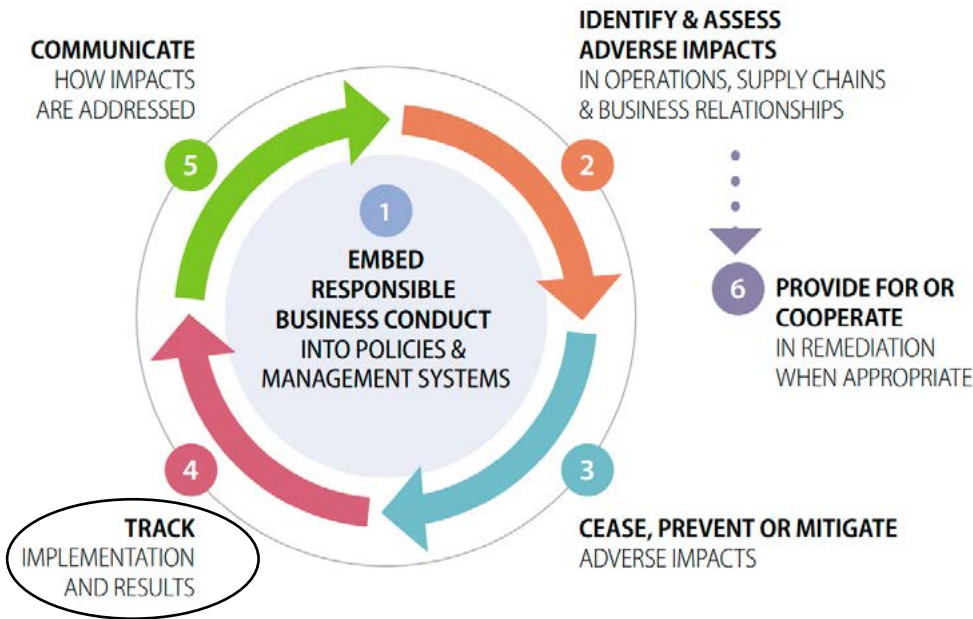
ZOOMING IN: remediation without expectation

Certain companies contribute to remediation, despite not being directly linked with or contributing to adverse human rights impacts. For instance, Fairphone, Signify, the Chinese cobalt refiner Huayou and the Impact Facility founded the FCA, whose mission is to improve working conditions in artisanal and small-scale cobalt mining. This MSI meanwhile includes downstream companies such as Google and Tesla, NGOs such as Save the Children and the Alliance for Responsible Mining, as well as mining companies such as Glencore and the Chinese CMOC. The FCA currently runs a project on a mining site near the city of Kolwezi in the DRC. They provide protection equipment to female miners for the washing of minerals and they support under-aged miners to return to school.

3.4 Tracking the effectiveness of actions

Once a company has started implementing mitigative actions, efforts should be made to track their implementation and results. In addition to efforts for monitoring a company’s own internal commitments, activities and goals, periodic assessments should be made of business relationships so as to ensure that progress is being made.¹⁰⁵

Figure 6: Due diligence according to the OECD – step 4 ‘track effectiveness’.



3.4.1 Audits

The primary mechanism through which companies have previously sought to monitor the extent to which business partners comply with human rights, including the expectations integrated into CoCs, is social audits. During a social audit, an auditor examines the documents provided by the company's management, conducts physical inspections of the workplace and interviews both management and (in some cases) workers. If violations are identified, the company being audited is typically expected to create and implement corrective actions.

ZOOMING IN: the Responsible Minerals Initiative and evolving auditing practices

One example is the **Responsible Minerals Initiative** (RMI), which currently has more than 500 member companies. Anticipating legislation in the US that will require conflict minerals to be disclosed, it was founded in 2008 (as the Conflict-Free Sourcing Initiative, or CFSI) by the Electronic Industry Citizenship Coalition and the Global e-Sustainability Initiative.¹⁰⁶ The RMI audits smelters and refiners of 3TG and cobalt, the so-called midstream segment of the supply chain, against its Responsible Minerals Assurance Process (RMAP) assessment standards and offers additional tools to help companies satisfy the requirements under US and EU due diligence legislation. In 2016, RMI also launched its Downstream Assessment Program (DAP), which applies to all minerals and caters to downstream companies (processors, traders and manufacturers) that are not eligible for the RMAP.¹⁰⁷ The DAP was recently updated after an OECD Alignment Assessment found significant discrepancies with OECD standards.¹⁰⁸

While social audits remain the mechanism of choice for monitoring human rights compliance, the auditing industry has also faced growing criticism. Common criticisms include potential conflicts of interest arising from the fact that auditors are often paid by auditees; the lack of transparency and accountability; a one-sided focus on the “paper reality” rather than the situation as it is on the ground, and a failure to involve (potentially) affected stakeholders meaningfully.¹⁰⁹ Auditing firms and standards-setting organisations have been slow to respond to these criticisms, although some efforts are being made to adopt more rigorous standards, enhance transparency and ensure that workers and communities have a greater voice in auditing practices. A particularly interesting evolution in this regard is the notion of “worker-driven social responsibility” (WSR), by which workers themselves are empowered to monitor the compliance of companies against human rights standards.

ZOOMING IN: Worker-driven social responsibility

WSR is built on the premise that affected stakeholders, notably workers at the base of global supply chains, should be empowered to monitor corporate compliance with human and labour rights standards. While WSR often involves audits, it also attempts to offer a response to the shortcomings of mainstream auditing systems. First, worker participation in the audit process is prioritised. Second, great care is taken to ensure confidentiality and employee safety (e.g., by organising interviews in “safe locations”). Third, more attention is paid to auditor training and auditors are required to master the local language.¹¹⁰

An interesting example of WSR is Electronics Watch (<http://www.electronicswatch.org>). This is an NGO that attempts to improve working conditions in electronics supply chains by bridging the gap

between public buyers, human rights experts and civil society in production countries. Specifically, Electronics Watch leverages an international network of monitoring partners, which invariably include NGOs, trade unions and other worker organisations. On the one hand, public buyers integrate the Electronics Watch CoC into their contracts with electronics suppliers. On the other, monitoring partners monitor compliance with this CoC. Monitoring methods are aimed at building trust with workers and at minimising the fear of reprisals for reporting abuses – for example, by carrying out off-site interviews. Findings and recommendations are reported in “compliance reports” that are used to stimulate a dialogue with companies and to ensure continuous improvement.

While social audits have mostly been a tool for monitoring upstream partners, some companies in the electronics industry are starting to integrate human rights concerns into their audits of sales partners.¹¹¹ This includes integrating a “right to verify” clause in their agreements with sales partners.

3.4.2 Technological solutions

While attention for sustainability continues to grow, innovations in digital technology create opportunities for more systematic assessment of human rights and environmental issues in global value chains. First, a growing number of companies are soliciting the support of specialised service providers such as EcoVadis, Sedex and IntegrityNext. Utilising extensive databases, big data analytics and artificial intelligence, they enable companies to comprehend much better how suppliers perform in the domain of sustainability. Ideally, these technologies could be applied to identifying human rights risks in downstream business relationships.

A second technology that is garnering a great deal of attention in the context of due diligence is blockchain. In essence, blockchain allows information to be stored and shared across a decentralised network of computers in a way that is secure, transparent and difficult to tamper with. Think of it as a digital notebook with different copies spread across a network. Each time a new transaction is registered by one of the users across the network, it is automatically added to every copy of the notebook, therefore ensuring that everyone has the same up-to-date record. Because of its setup, it is difficult to tamper with the information without everyone else noticing. In theory, this immutability of data, combined with decentralised verification, makes blockchain a trustworthy and reliable instrument with which to ensure supply chain transparency.¹¹²

ZOOMING IN: Blockchain—promises and pitfalls

Many of the erstwhile initiatives involving blockchain emerged from the food industry. One example is the IBM Food Trust initiative. Launched in 2016, the Food Trust brings together a broad range of stakeholders from across the food industry, including growers, processors, wholesalers, distributors, manufacturers, retailers and consumers. The rationale behind the IBM Food Trust is to use blockchain technology to create a secure, transparent and immutable ledger of food system data that can be accessed by various parties in the supply chain. While experiences so far suggest clear gains in supply chain transparency, the implementation of the IBM Food Trust also reveals key challenges. These include the need for close collaboration and coordination across diverse stakeholders, ensuring regulatory compliance across different jurisdictions, and fostering trust in blockchain technology.¹¹³

Another IBM blockchain initiative is designed for the DRC's cobalt sector, where miners often face harsh conditions. Cobalt is a mineral used by the automotive and electronics industries to make lithium-ion batteries for electric vehicles, smartphones and laptops. The Responsible Sourcing Blockchain Network (RSBN), built on the IBM Blockchain Platform, aims to provide transparency and security in demonstrating responsible sourcing practices. The network should ensure an immutable audit trail and secure the storage of provenance information, enabling companies to prove ethical production.¹¹⁴ However, the RSBN is designed "to keep cobalt mined by hand out of companies' supply chains" instead of allowing for constructive cooperation with the artisanal cobalt sector.

A good example of a constructive blockchain initiative is a platform developed by Consensus, a Canadian tech company. The platform is adapted to the capabilities available in the artisanal mining sector and is being deployed in the Just Gold programme of Canadian NGO IMPACT.¹¹⁵ Just Gold focuses on mining in Ituri, a province in eastern DRC. It allows companies to source artisanal gold confidently from the DRC while supporting upstream supply chain actors progressively to meet international market standards.

While some interesting examples of blockchain use can be identified, it continues to face important challenges.¹¹⁶ First, there may be technical challenges (notably in developing countries) related to the availability of network infrastructure. Second, the costs of and technical expertise required for blockchain solutions may raise barriers to entry, notably for smaller firms. Third, and most importantly, the effectiveness of blockchain depends not only on the willingness and capacity of actors to collect data and feed these into the system, but also on the quality and integrity of the data. This creates clear risks for human error or even for intentional manipulation. Overall, the potential of blockchain to facilitate more sustainable supply chains has largely remained unproven. Existing "best practices" mostly focus on realising end-to-end transparency, which enables tracing the movement of goods without monitoring the social or environmental circumstances in which these goods are produced.



Monitoring impacts: relevant lessons for the defence industry

Companies in the sectors we examined commonly use auditors to verify the human rights compliance of business partners. The previous section highlights a number of caveats surrounding this practice, including the fact that it has mainly been applied in an upstream context. While WSR may be a promising approach to monitoring working conditions in supply chains, it is not easily applicable to downstream due diligence in the defence industry. Nonetheless, interviewees from the defence industry indicated that the employees of some defence contractors – notably those who are also involved in other sectors aside from defence – also care about their employer’s ethical behaviour and could become more involved in due diligence processes.

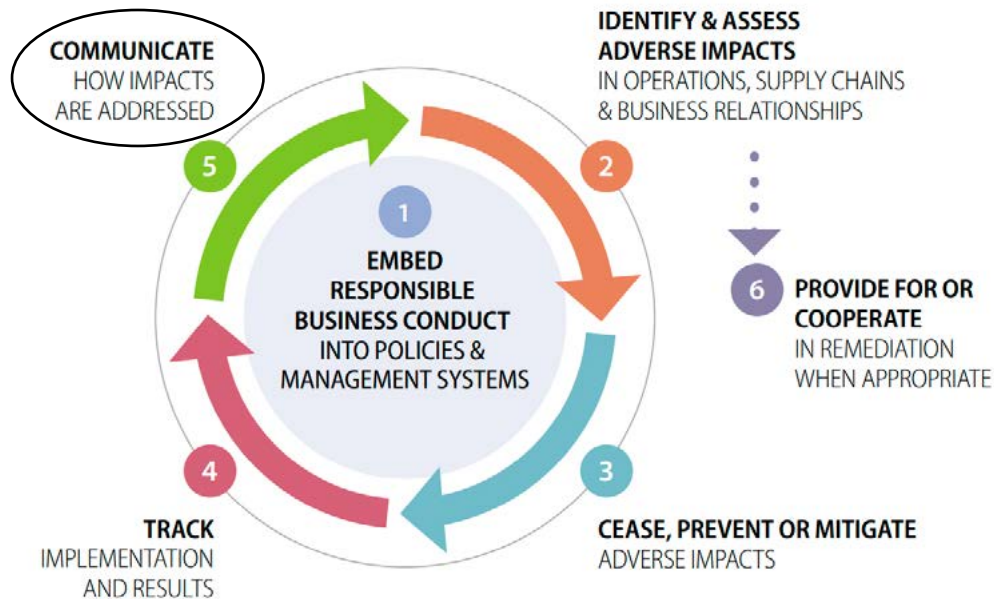
It should also be noted that some governments – for example, Germany – carry out on-site inspections to verify the end-use of their licensed arms exports. During the Eighth ATT Conference of the States Parties in 2022, post-shipment controls, including on-site inspections, were a central theme, with several papers addressing the challenges involved in these processes. These challenges include difficulties in securing access to importing countries and also ensuring the effectiveness of inspections. For a more detailed exploration of these challenges, several resources provide insights, such as SIPRI’s briefing papers on post-shipment controls and on-site inspections, which outline the complexities of conducting such checks and their importance to verifying end-use compliance.¹¹⁷

Companies in the defence sector are increasingly turning to technological solutions to respond to compliance issues and effect customer screening. There is a growing need for tools to screen constantly evolving sanctions lists which pertain not only to human rights concerns, but also to corruption, drugs and other factors. Regarding blockchain, the same scepticism prevails as in other industries (“rubbish in, rubbish out”).

3.5 Communicating due diligence

According to the OECD, public reporting is an integral aspect of due diligence. Communication must include information on all aspects of due diligence, ranging from policies and the results of risk assessments to the actions taken to mitigate impacts and also the results of such mitigating activities. Historically, sustainability reporting has mostly been a voluntary affair and many companies are reluctant to share detailed and verifiable information on the human rights impacts of their products and services. When they do report, companies tend to mirror each other’s reporting habits in order not to stand out.¹¹⁸ Whereas the available evidence suggests that there has been a notable increase in reporting on human rights in recent years, only a minority of companies are actively and systematically reporting on their due diligence processes.¹¹⁹

Figure 7: Due diligence according to the OECD – step 5 'communicate due diligence'.



However, there are good reasons to expect change in the coming years. On the one hand, leading (albeit voluntary) sustainability standards such as those of the Global Reporting Initiative (GRI) are increasingly integrating reporting requirements related to human rights and due diligence¹²⁰ into their business practices. The sustainability reports of companies that follow GRI reporting standards are accordingly able to offer practical guidance on how to report on human rights issues. On the other hand, the European CSRD signals a shift towards mandatory reporting. Under the CSRD, companies will not only have to disclose their (potential) impacts on human rights, but will also have to report on their policies and actions taken to manage these impacts (including due diligence processes). But while the EU has developed elaborate (but also highly complex) guidance on how companies should carry out a double materiality assessment and should approach the matter of value chains, practical examples of CSRD-compliant reporting are limited.

Reporting: lessons for the defence industry

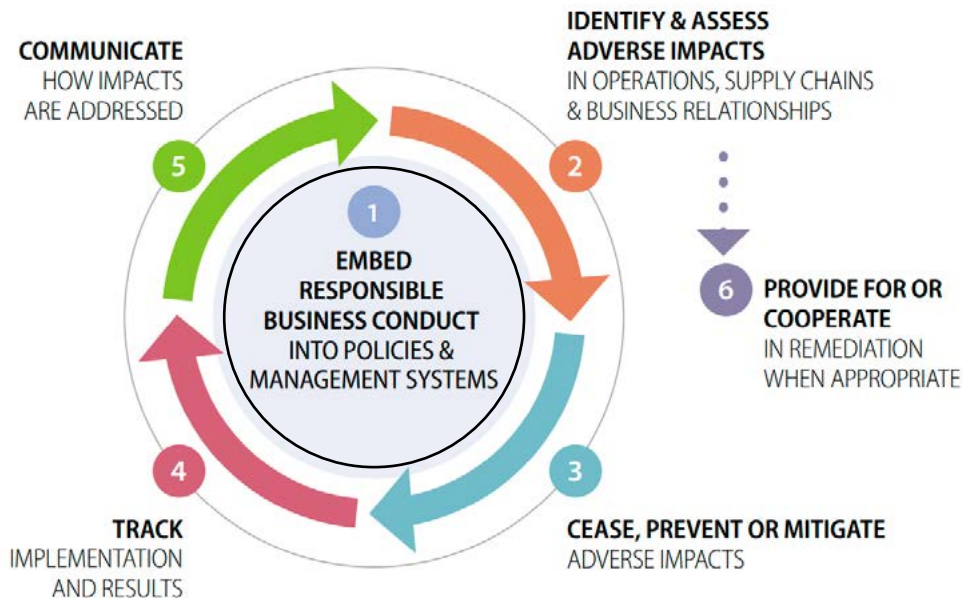
Unlike the CS3D (due diligence), the CSRD applies fully to defence companies. This includes not just large companies based in the EU, but also non-European companies with a significant turnover in the EU. In practice, like companies in other sectors, companies in the defence industry will be expected to undertake a "double materiality assessment", namely, an analysis aimed at determining their relevant sustainability impacts across several sustainability topics. One of these topics (described in standard ESRS S3) deals specifically with impacts on affected communities. First, companies will have to decide whether, through the sale or use of their goods, they could become linked to material impacts on aspects such as the security, privacy or freedom of expression of communities. Second, companies will have to disclose the policies they have in place and the practical steps they are taking to manage these impacts. At the same time, it is important to remember that the CSRD contains only a reporting obligation and does not oblige companies to take action. In theory, companies could disclose non-action – although in practice it will be difficult for those that disclose negative impacts to say that they are not doing anything to reduce or reverse those impacts.

3.6 Policy integration

To ensure that due diligence becomes structurally embedded in business operations, companies should develop, adopt and disseminate policies that articulate their commitments to due diligence. Moreover, oversight of and responsibility for due diligence need to be clearly assigned in the business or organisation.¹²¹

The UNGPs and the OECD Guidelines expect businesses to make a clear policy commitment to human rights and to implementing due diligence. This commitment should be approved by management; it should stipulate the business's expectations of its personnel, its business partners, and any other relevant stakeholders; and it should be publicly available and communicated.¹²² It can be a standalone commitment, but ideally it should form part of a broader integrated due diligence policy that speaks to the different processes that were discussed in this report. The available evidence suggests that, while a growing number of companies are adopting formal policy commitments, in most cases these policy commitments do not yet form part of more holistic due diligence policies.¹²³ However, the food industry may offer a glimpse into what holistic due diligence policies could look like.

Figure 8: Due diligence according to the OECD – ‘embed into policies’.



Ahold Delhaize elaborates on its due diligence strategy on its website and publishes elaborate human rights reports that detail the way this strategy is put into practice

ZOOMING IN: Food retail – towards integrated due diligence policies

Food retailers occupy a unique position in global food supply chains, interacting as they do with both end-consumers and a wide variety of businesses in the agricultural sector and the food industry. As a consequence, they are not only linked to a wide range of (potential) human rights impacts, but also face a unique set of pressures to engage with these risks. Responding to these pressures, major food retailers are in the process of adopting more holistic human rights policies. Consider, for instance, the case of Lidl. In 2018, it was among the lowest-scoring companies in an Oxfam report on the human rights efforts of supermarkets.¹²⁴ This report was one of the key incentives for Lidl to start developing elaborate human rights policies and generating regular human rights progress updates. These updates contain a series of commitments but they include concrete actions through which the retailer seeks to redress (potential) adverse impacts in its global supply chains.¹²⁵ Similarly, Ahold Delhaize elaborates on its due diligence strategy on its website and publishes elaborate human rights reports that detail the way this strategy is put into practice.¹²⁶

Policy integration: lessons for the defence industry

Many major defence companies are now putting in place human rights policies, but not all of them are publicly available. Moreover, only a few of these policies explicitly reference the UNGPs or the OECD Guidelines; consequently, it is difficult to find specific details about due diligence provisions in the defence industry.¹²⁷ Amid increasing societal and investor expectations, though, defence undertakings could explore the innovative practices in other industries. Their commitment to human rights (due diligence) should be approved by management; should stipulate the business's expectations towards its personnel, its business partners and other relevant stakeholders, and should be available and communicated publicly.

Conclusion

Attention to responsible business conduct is gaining ground. Faced with the prospect of new sustainability reporting and due diligence legislation, and with increasing client and investor pressures, companies across industries are gradually starting to implement due diligence processes in order to identify and mitigate human rights impacts and to communicate such impacts on human rights and the environment. The defence industry, which has long operated under the assumption that government export controls would suffice in this regard, is no longer insulated from these pressures.

In this report, we have taken a closer look at the practical implications of these trends. How can the defence industry effectively integrate HRDD into its members' existing practices? In this respect, what challenges do defence businesses face? What lessons can be learned from other sectors that are faced with similar challenges? In this concluding chapter, we attempt to summarise the key lessons that have emerged from our analysis.

Lesson 1: The defence industry is not unique

Defence companies undoubtedly encounter important challenges when conducting due diligence, including a lack of transparency in the arms value chain and the fact that the most severe risks are situated downstream – related to the (mis)use of weapons – rather than in the upstream supply chain. However, these challenges are not unique to the defence industry. Similar difficulties are encountered by companies in other sectors, such as extractives and digital technology. In these sectors, too, complex supply chains and the downstream impacts of products also present substantial hurdles in implementing effective due diligence.

Lesson 2: Existing mechanisms fall short of due diligence standards

Whereas both regulators and the defence industry have taken steps to prevent arms from being misused, these actions – such as government export controls and licensing procedures – are not a substitute for comprehensive due diligence. Unlike other sectors,

such as minerals, where established frameworks like the OECD Due Diligence Guidance for responsible supply chains of minerals from conflict-affected and high-risk areas outline clear risk indicators, the arms industry lacks similarly detailed guidelines. This gap leaves companies facing ethical dilemmas in assessing human rights risks, such as sales to regimes with poor human rights records or those engaged in repression. Without clear standards, many defence companies rely solely on government controls, which are not designed to deal fully with broader human rights concerns. There is therefore a pressing need for more nuanced and proactive due diligence processes to be introduced to ensure that companies can assess the full range of downstream risks and take preventive measures to avoid contributing to human rights abuses.

Lesson 3: There are lessons to be learned from other industries, but customisation is required

The extractives and technology sectors are developing several practices that the defence industry could build upon. Leading tech companies, such as HPE and Ericsson, are setting a precedent by systematically mapping downstream risks and integrating human rights safeguards into sales contracts, licences and service agreements. While similar practices already exist in the defence industry – such as the use of regulatory, non-re-exportation and hardship clauses – there is room to expand these safeguards further by drawing on the experiences of the tech and extractives sectors. However, regarding monitoring, the defence industry faces unique challenges. Tools such as audits and blockchain, which already have limitations in other industries, may be even less effective in the defence sector due to the sector's complexity and sensitivity. This underscores the need for more tailored monitoring mechanisms that reflect the specific risks inherent in the arms trade.

Lesson 4: The indispensable role of responsible public procurement

The defence industry operates under a unique dynamic by which governments, as primary clients, set the rules of the game. Paradoxically, however, the standards imposed by public buyers often fall short of those set by private businesses (in, e.g., B2B relationships). This inconsistency, which is certainly not unique to the defence industry, leads to frustration on the part of companies. According to the UNGPs, a state's duty to protect human rights also extends to public procurement. Any meaningful progress in this area will require active government involvement and a commitment to higher standards.

Lesson 5: The power of collective action

Individual defence companies often have limited leverage over their business partners, which makes collective action within the industry crucial. By collaborating, companies are able to create a stronger, more unified push toward higher standards. Building on existing institutions, such as industry associations and multilateral initiatives, could provide a valuable foundation for these efforts. However, while industry-driven initiatives could lay a strong foundation for collective action, the involvement of other

key stakeholders – governments, civil society and international organisations – will be key to ensuring the effectiveness and credibility of due diligence efforts.

In the current geopolitical context, the defence industry will continue to play a pivotal role in ensuring national and international security. However, this permanence comes with an important responsibility: the need to ensure that the industry adheres to internationally agreed principles regarding responsible business conduct and respect for human rights. Achieving this will require all stakeholders – governments, industry leaders, civil society and international organisations – to move past longstanding divisions and collaborate to find common ground. This collaborative effort must focus on minimising human suffering by establishing and enforcing ethical standards across the board. The path forward will be challenging, but the stakes are too high to allow for inaction or continuing division to persist.



Endnotes

- 1 United Nations Human Rights Office of the High Commissioner, 'Guiding principles on business and human rights. Implementing the United Nations "Protect, Respect and Remedy" Framework' (2011) 18. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf
- 2 OECD, 'OECD guidelines for multinational enterprises on responsible business conduct' (2023). <https://doi.org/10.1787/81f92357-en>.
- 3 The hyperlinks below were last verified on 23 May 2024. Machito Kanetake & Cedric Ryngaert, 'Due diligence and corporate liability of the defense industry: Arms exports, end use and corporate responsibility' (Flemish Peace Institute, 2023). <https://vlaamsvredesinstituut.eu/en/report/due-diligence-and-corporate-liability-of-the-defense-industry-arms-exports-end-use-and-corporate-responsibility/>
- 4 Arms Trade Treaty, Final report of the ninth conference of State Parties (ATT/CSPg/2023/SEC/773/Conf.FinRep.Rev2). https://thearmstradetreaty.org/hyper-images/file/ATT_CSPg_ATT_S_Final%20Report_%20rev2_EN/ATT_CSPg_ATT_S_Final%20Report_%20rev2_EN.pdf.
- 5 OECD, 'OECD guidelines for multinational enterprises on responsible business conduct' (2023). <https://doi.org/10.1787/81f92357-en>.
- 6 OECD, 'OECD due diligence guidance for responsible business conduct' (2018). <https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf>
- 7 Ibid.
- 8 The OECD's initial guidelines showed some ambiguity regarding downstream impacts. However, the latest version of the guidelines clearly states that due diligence obligations apply to the entire value chain, including the entire downstream (see footnote 2).
- 9 Almut SchillingVacaflor & Andrea Lenschow, 'Hardening foreign corporate accountability through mandatory due diligence in the European Union? New trends and persisting challenges' (2023) *Regulation & Governance*, 17, 3: 677–693. <https://doi.org/10.1111/rego.12402>
- 10 Amélie Férey & Laure de Roucy-Rochegonde, "Don't bank on the bombs". New European Standards Affecting the Defense Industry' (IFRI, 2022). https://www.ifri.org/sites/default/files/atoms/files/ferey_deroucyrochegonde_dont_bank_on_the_bombs_2022.pdf
- 11 European Commission (2023). Commission Delegated Regulation (EU) 2023/2772, paragraph 40(d), page 48. In supplementing Directive 2013/34/EU of the European Parliament and of the Council as regards sustainability reporting standards. Official Journal of the European Union, L 2023/2772.
- 12 IPIS/VUB, 'Due diligence and corporate accountability in the arms value chain' (2024) 53. https://ipisresearch.be/wp-content/uploads/2024/03/20240327_Due-diligence-and-corporate-accountability-in-the-arms-value-chain.pdf
- 13 Karina Fernandez-Stark & Gary Gereffi, 'Global value chain analysis: A primer' *Handbook on global value chains* (Edward Elgar Publishing, 2019) 54–76. https://www.researchgate.net/publication/337170997_Global_value_chain_analysis_a_primer_second_edition
- 14 T.A. Gardner et al., 'Transparency and sustainability in global commodity supply chains' (2019) *World Development*, 121: 163–177. <https://www.sciencedirect.com/science/article/pii/S0305750X18301736>
- 15 Human Rights Watch, 'Sparkling jewels, opaque supply chains. Jewelry companies, changing sourcing practices, and Covid-19' (2020). <https://www.hrw.org/report/2020/11/24/sparkling-jewels-opaque-supply-chains/jewelry-companies-changing-sourcing>
- 16 Meaghan Malloy, 'Addressing adverse human rights impacts connected to product misuse. A good practice note endorsed by the United Nations Global Compact Human Rights and Labour Working Group on 31 May 2017' (2017). <https://unglobalcompact.org/library/5311>
- 17 UN Working Group on Business and Human Rights, 'Responsible business conduct in the arms sector: Ensuring business practice in line with the UN Guiding Principles on Business and Human Rights' (2022). <https://www.ohchr.org/sites/default/files/2022-08/BHR-Arms-sector-info-note.pdf>
- 18 IPIS/VUB, 'Due diligence and corporate accountability in the arms value chain' (2024). https://ipisresearch.be/wp-content/uploads/2024/03/20240327_Due-diligence-and-corporate-accountability-in-the-arms-value-chain.pdf
- 19 See, notably, Eian Katz, 'Defense industry human rights due diligence guidance' (American Bar Association Center for Human Rights, 2022) 6. https://www.americanbar.org/groups/human_rights/reports/defense-industry-human-rights-due-diligence-guidance/
- 20 Ibid.
- 21 SIPRI, 'Yearbook 2023. Armaments, disarmament and international security. Summary' (2023) 22–23. https://www.sipri.org/sites/default/files/2023-06/yb23_summary_en_0.pdf
- 22 For example, UK Finance & ADS Group, 'Guide for the defense and security sectors on access to financial services in the UK' (December 2023) 6. <https://www.ukfinance.org.uk/system/files/2023-12/Defense%20and%20Security%20Access%20to%20finance%20guide.pdf>

- 23 Eian Katz, 'Defense industry human rights due diligence guidance' (American Bar Association Center for Human Rights, 2022) 5. https://www.americanbar.org/groups/human_rights/reports/defense-industry-human-rights-due-diligence-guidance/
- 24 Hiruni Alwishewa, 'The move towards human rights due diligence policies by the arms industry' (Forum on the Arms Trade, 18 January 2024). <https://www.forumarmstrade.org/blog/the-move-towards-human-rights-due-diligence-policies-by-the-arms-industry>; UN Working Group on Business and Human Rights, 'Responsible business conduct in the arms sector: Ensuring business practice in line with the UN Guiding Principles on Business and Human Rights' (2022) 6. <https://www.ohchr.org/sites/default/files/2022-08/BHR-Arms-sector-info-note.pdf>
- 25 Eian Katz, 'Defense industry human rights due diligence guidance' (American Bar Association Center for Human Rights, 2022) 6. https://www.americanbar.org/groups/human_rights/reports/defense-industry-human-rights-due-diligence-guidance/
- 26 For example, US Securities and Exchange Commission, 'The Franciscan Sisters of Allegany, NY (the "Proponent") urges shareholders to vote FOR Proposal 5, the shareholder proposal requesting a report on human rights due diligence, at the General Dynamics Corporation Annual Meeting of Shareholders on May 4, 2022' (2022). <https://www.sec.gov/Archives/edgar/data/1636143/000121465922005902/r427222px14a6g.htm>; Triodos Investment Management, 'Investing in arms is not sustainable' (13 April 2022). <https://www.triodos-im.com/articles/2022/triodos-position-on-investing-in-arms>
- 27 Eian Katz, 'Defense industry human rights due diligence guidance' (American Bar Association Center for Human Rights, 2022) 7. https://www.americanbar.org/groups/human_rights/reports/defense-industry-human-rights-due-diligence-guidance/
- 28 Cor Oudes, Frank Slijper & Michel Uiterwaal, 'High-risk arms trade and the financial sector' (PAX, 2022). <https://paxforpeace.nl/news/largest-european-banks-bankroll-high-risk-arms-traders/>
- 29 See, for instance, Vredesactie/IPIS, 'Belgische wapenexport naar Israël: De speling tussen woord en daad in het exportcontrolebeleid' (2024). <https://ipisresearch.be/publication/belgian-arms-exports-to-israel-the-discrepancy-between-words-and-deeds-in-export-control-policy/>
- 30 Machito Kanetake & Cedric Ryngaert, 'Due diligence and corporate liability of the defense industry: Arms exports, end use and corporate responsibility' (Flemish Peace Institute, 2023) 39. <https://vlaamsvredesinstituut.eu/en/report/due-diligence-and-corporate-liability-of-the-defense-industry-arms-exports-end-use-and-corporate-responsibility/>
- 31 For a non-exhaustive overview of the case law on corporate accountability in arms value chains, see IPIS/VUB, 'Due diligence and corporate accountability in the arms value chain' (2024) 44–46 and annexures. https://ipisresearch.be/wp-content/uploads/2024/03/20240327_Due-diligence-and-corporate-accountability-in-the-arms-value-chain.pdf; for a general list of arms-trade-related case law: <https://armstradelitigationmonitor.org/>.
- 32 Eian Katz, 'Defense industry human rights due diligence guidance' (American Bar Association Center for Human Rights, 2022) 10. https://www.americanbar.org/groups/human_rights/reports/defense-industry-human-rights-due-diligence-guidance/
- 33 For a summary of the various arguments and counterarguments in the literature on the justification for companies to make ethical, strategic, and geopolitical assessments, see IPIS/VUB, 'Due diligence and corporate accountability in the arms value chain' (2024) 53. https://ipisresearch.be/wp-content/uploads/2024/03/20240327_Due-diligence-and-corporate-accountability-in-the-arms-value-chain.pdf 8–9.
- 34 Ibid.
- 35 Amnesty International, 'Outsourcing responsibility: Human rights policies in the defense sector' (2019) 23. <https://www.amnesty.org/en/documents/act30/0893/2019/en/>; <https://www.amnesty.org/en/documents/act30/0893/2019/en/>; Machito Kanetake & Cedric Ryngaert, 'Due diligence and corporate liability of the defense industry: Arms exports, end use and corporate responsibility' (Flemish Peace Institute, 2023). <https://vlaamsvredesinstituut.eu/en/report/due-diligence-and-corporate-liability-of-the-defense-industry-arms-exports-end-use-and-corporate-responsibility/>
- 36 Hiruni Alwishewa, 'Responsibilities to prevent: Responsibilities of supply-side actors to prevent the adverse human rights impacts of arms exports to conflict zones. Thesis submitted to the Graduate Institute of International and Development Studies, Geneva' (2024) 156–157. <https://repository.graduateinstitute.ch/record/302662?v=pdf>
- 37 Interview with a representative of a European defence company, 11.7.2024; interview with a representative of a European defence company, 22.7.2024.
- 38 UN Working Group on Business and Human Rights, 'Responsible business conduct in the arms sector: Ensuring business practice in line with the UN Guiding Principles on Business and Human Rights. Information Note by the UN Working Group on Business and Human Rights' (2022) 6. <https://www.ohchr.org/sites/default/files/2022-08/BHR-Arms-sector-info-note.pdf>
- 39 Kongsberg, 'Human rights report' (2022) 15. <https://digitallibrary.un.org/record/694127?ln=en&v=pdf>
- 40 Canadian Commercial Corporation, 'Human rights due diligence guidelines. defense and security' (2019). <https://www.ccc.ca/wp-content/uploads/2019/12/9.-CCC-Human-Rights-Due-Diligence-Guidelines-Defense-Security.pdf>; Canadian Commercial Corporation, 'Human rights due diligence instruction' (2019). <https://www.ccc.ca/wp-content/uploads/2019/12/10.-CCC-Human-Rights-Due-Diligence-Instructions.pdf>
- 41 Flanders Chancellery and Foreign Office/Strategic Goods Control Unit, 'Export control responsibilities & human rights due diligence. Government of Flanders' practical approach' (ATT CSP10 WGETI, 21 February 2024). https://www.thearmstradetreaty.org/hyper-images/file/Government%20of%20Flanders%20-%20ATT_CSP10_WG%20meetings_Day%201-2_WGETI_Current%20and%20emerging%20issues_Industry/Government%20of%20Flanders%20-%20ATT_CSP10_WG%20

meetings_Day%201-2_WGETI_Current%20and

- 42 Participating States of the Wassenaar Arrangement, 'Best practice guidelines on internal compliance programmes for dual-use goods and technologies' (2011).
- 43 European Commission, 'Recommendation (EU) 2019/1318 of 30 July 2019 on internal compliance programmes for dual-use trade controls under Council Regulation (EC) No 428/2009'.
- 44 See, e.g., the Export Controls and Human Rights Initiative launched at the Summit for Democracy (an initiative by the US presidency bringing together governments, civil society and the private sector) in March 2023 and its 'Code of conduct for enhancing export controls of goods and technology that could be misused and lead to serious violations or abuses of human rights' (2023). <https://www.state.gov/wp-content/uploads/2023/03/230303-Updated-ECHRI-Code-of-Conduct-FINAL.pdf>.
- 45 Austria, Ireland, Mexico, 'Joint working paper: Responsible business conduct and the Arms Trade Treaty' (ATT/CSP9/2023/AUT-IRL-MEX/774/Conf.WP, 10 August 2023). https://www.thearmstradetreaty.org/hyper-images/file/ATT_CSP9_Austria,%20Ireland,%20Mexico_Joint%20Working%20Paper_Responsible%20Business%20Conduct%20and%20the%20Arms%20Trade%20Treaty/ATT_CSP9_Austria,%20Ireland,%20Mexico_Joint%20Working%20Paper_Responsib
- 46 Arms Trade Treaty Working Group on Effective Treaty Implementation, 'Tenth Conference of States Parties' (ATT/CSP10.WGETI/2024/CHAIR/775/LetterSubDocs, 22 January 2024) 62. https://www.thearmstradetreaty.org/hyper-images/file/ATT_WGETI_CSP10_Chair%20Letter%20and%20Sub-WG%20Documents%20for%2020-21%20February%202024_EN/ATT_WGETI_CSP10_Chair%20Letter%20and%20Sub-WG%20Documents%20for%2020-21%20February%202024_EN.pdf
- 47 Technologies Accountability Project, 'Navigating the surveillance technology ecosystem: A human rights due diligence guide for investors' (2022). https://media.business-humanrights.org/media/documents/2022_STAP_Guide_v5.pdf
- 48 UN Security Council, 'Letter dated 15 November 2010 from the Chair of the Security Council Committee established pursuant to resolution 1533 (2004) concerning the Democratic Republic of the Congo addressed to the President of the Security Council' (UNSC/2010/596). Kongsberg, 'Human rights report' (2023) 7. https://www.kongsberg.com/contentassets/8363852a2df844018bdd1d46bc640e0e/kog_humanrights_23_290524.pdf
- 49 UN Security Council, 'Due diligence guidelines' (s.d.). <https://www.un.org/securitycouncil/sanctions/1533/due-diligence-guidelines>
- 50 IPIS, 'Guide to current mining reform initiatives in eastern DRC' (2011) 6. <https://ipisresearch.be/publication/guide-current-mining-reform-initiatives-eastern-drc/>
- 51 IPIS, 'Evaluating due diligence programs for conflict minerals' (2021). <https://ipisresearch.be/publication/evaluating-due-diligence-programs-for-conflict-minerals/>
- 52 OECD, 'OECD due diligence guidance for responsible supply chains of minerals from conflict-affected and high-risk areas. Third Edition' (2016). <http://dx.doi.org/10.1787/9789264252479-en>.
- 53 European Commission/Trade, 'Conflict Minerals Regulation: The regulation explained' (s.d.). https://policy.trade.ec.europa.eu/development-and-sustainability/conflict-minerals-regulation/regulation-explained_en#:~:text=The%20Conflict%20Minerals%20Regulation%20aims,are%20mined%20using%20forced%20labour.
- 54 OECD, 'Monitoring corporate disclosure. Assessing company reporting on mineral supply chain due diligence' (2022) 6. <https://mneguidelines.oecd.org/monitoring-corporate-disclosure-assessing-company-reporting-on-mineral-supply-chain-due-diligence.pdf>
- 55 OECD, 'OECD due diligence guidance for responsible supply chains of minerals: Resources' (s.d.). <https://mneguidelines.oecd.org/responsible-mineral-supply-chain-resources.htm>
- 56 Global Witness, 'Conflict diamonds' (s.d.). <https://www.globalwitness.org/en/campaigns/conflict-diamonds/>
- 57 Kimberley Process, 'What is the Kimberley Process?' (s.d.). <https://www.kimberleyprocess.com/en/what-kp>; <https://www.kimberleyprocess.com/en/2003-kpcs-core-document>
- 58 The KP certification scheme (KPCS) differs from due diligence schemes in that it is government-led, not company-led, and does not employ the notion of 'gradual improvement' in assessing companies' implementation. The latter concerns diamond companies' compliance with administrative procedures outlined in domestic laws and regulations. For example, in the CAR, diamond exporters seeking certification of their parcels must submit documentary proof to the country's KP authority that their stones were mined in a zone not controlled by rebels.
- 59 For example, De Beers Group, 'Best practice principles assurance programme' (s.d.). <https://www.debeersgroup.com/sustainability-and-ethics/leading-ethical-practices-across-the-industry/best-practice-principles-assurance-programme>; Signet Jewelers, 'Responsible sourcing' (s.d.). <https://www.signetjewelers.com/sustainability/responsible-sourcing/default.aspx>
- 60 Responsible Jewellery Council, 'Watches, jewellery & sustainability' (s.d.). <https://www.responsiblejewellery.com/>
- 61 Bain & Company and Antwerp World Diamond Centre, 'The global diamond industry 2019' (2019) 3. https://www.bain.com/contentassets/e225bceffd7a48b5b450837adbbfee88/bain_report_global_diamond_report_2019.pdf
- 62 Financial Action Task Force, 'Money laundering and terrorist financing through trade in diamonds' (s.d.). <https://www.fatf-gafi.org/en/publications/Methodsandrends/ML-tf-through-trade-in-diamonds.html>
- 63 IPIS, 'Belgium's fight against conflict diamonds: An assessment of the country's diamond sector controls from a global perspective' (2021) 57-59. <https://ipisresearch.be/publication/belgiums-fight-against-conflict-diamonds-an-assessment-of-the-countrys-diamond-sector-controls-from-a-global-perspective/>

- 64 OECD, 'OECD due diligence guidance for responsible business conduct' (2018) 25. <https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf>
- 65 Ericsson, '5G human rights assessment' (2021). <https://www.ericsson.com/49295a/assets/local/about-ericsson/sustainability-and-corporate-responsibility/documents/2021/5g-human-rights-assessment---final.pdf>
- 66 Business for Social Responsibility (BSR), 'Human rights due diligence of products and services assessing the downstream value chain' (2021). <https://www.bsr.org/reports/BSR-Human-Rights-Due-Diligence-Products-Services.pdf>
- 67 Institute for Human Rights, 'Due diligence in the downstream value chain. Case studies of current company practice' (Revised version, 2023) 18. <https://www.humanrights.dk/publications/due-diligence-downstream-value-chain-case-studies-current-company-practice>
- 68 Hewlett Packard, 'HPE human rights report' (2022). https://www.hpe.com/psnow/doc/a50008837enw?jumpid-in_pdfviewer-psnow
- 69 BSR, 'Human rights due diligence of products and services assessing the downstream value chain' (2021) 4. <https://www.bsr.org/reports/BSR-Human-Rights-Due-Diligence-Products-Services.pdf>
- 70 PWC, 'Know your customer's ESG risks. Why ESG should be part of a financial institution's customer due diligence process' (s.d.). [pwc-know-your-customer-esg-risks.pdf](https://www.pwc.com/kyc/kyc-know-your-customer-esg-risks.pdf)
- 71 Antwerp World Diamond Centre, 'Bureau van Dijk database' (s.d.). <https://www.awdc.be/en/KYC>
- 72 Bureau van Dijk is a Moody's Analytics company. In January 2024, the US credit rating agency retired the bureau's website and dropped its name. The business data resource tool now goes under the name of Orbis.
- 73 OECD, 'OECD due diligence guidance for responsible business conduct' (2018) 28. <https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf>
- 74 United Nations Human Rights Office of the High Commissioner, 'Guiding principles on business and human rights. Implementing the United Nations "Protect, Respect and Remedy" Framework' (2011) 18. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf
- 75 Shift, 'Using leverage in business relationships to reduce human rights risks' (2013). https://shiftproject.org/wp-content/uploads/2013/11/Shift_leverageUNGPs_2013.pdf
- 76 Ardea International, 'The value of supplier codes of conduct: Supporting transparency and improving performance' (2020) 13. <https://www.ardeainternational.com/resources/publications/the-value-of-supplier-codes-of-conduct/>
- 77 Meaghan Malloy, 'Addressing adverse human rights impacts connected to product misuse. A good practice note endorsed by the United Nations Global Compact Human Rights and Labour Working Group on 31 May 2017' (2017). <https://unglobalcompact.org/library/5311>
- 78 Hewlett Packard, 'Partner code of conduct' (Revised version, 2023). <https://www.hpe.com/psnow/doc/a00042891enw>
- 79 IPIS/Solidaridad, 'Due diligence and the risk of disengagement: Experiences from the mineral sector and a way forward for the CSDDD' (2023) 3. <https://ipisresearch.be/publication/due-diligence-and-the-risk-of-disengagement-experiences-from-the-mineral-sector-and-a-way-forward-for-the-csddd/>
- 80 Somo, 'Should I stay or should I go? Exploring the role of disengagement in human rights due diligence' (April 2016). <https://www.somo.nl/download/40571/?tmstv-1717435074>
- 81 Maytaal Angel & Bernadette Christina, 'Nestlé to stop sourcing from Indonesian palm oil producer AAL'. Reuters, 1 October 2022. <https://www.reuters.com/business/sustainable-business/nestle-stop-sourcing-indonesian-palm-oil-producer-aal-2022-09-30/>
- 82 Jeff Blagdon, 'Apple cuts ties with supplier after audit reveals 74 cases of underage labor'. *The Verge*, 25 January 2013. <https://www.theverge.com/2013/1/25/3914252/apple-severs-ties-with-supplier-after-audit-reveals-74-cases-of>
- 83 Meaghan Malloy, 'Addressing adverse human rights impacts connected to product misuse. A good practice note endorsed by the United Nations Global Compact Human Rights and Labour Working Group on 31 May 2017' (2017). <https://unglobalcompact.org/library/5311>
- 84 *The East African*, 'Eacop's financing blues as lenders desert \$3.5b project' (4 May 2021). <https://www.theeastafrican.co.ke/tea/business/eacop-financing-blues-3385942>
- 85 For more background see: <https://burmacampaign.org.uk/newtec/>
- 86 Shift, 'From policing to partnership. Designing an EU due diligence duty that delivers better outcomes' (2023). <https://shiftproject.org/wp-content/uploads/2023/05/Policing-to-Partnership-May-2023.pdf>
- 87 Apple, 'Supply chain innovation reports' (s.d.). <https://www.supplychainreports.apple/home/default.aspx> https://www.apple.com/supplier-responsibility/pdf/Apple_SR_2023_Progress_Report.pdf
- 88 Business & Human Rights Resource Centre, 'China: Apple accused of violating labour laws as employees at iPhone factory found working 100 hours of overtime & being "punished" for not meeting targets' (9 September 2019). <https://www.business-humanrights.org/en/latest-news/china-apple-accused-of-violating-labour-laws-as-employees-at-iphone-factory-found-working-100-hours-of-overtime-being-punished-for-not-meeting-targets-incl-co-comments/>
- 89 BSR, 'Human rights due diligence of products and services assessing the downstream value chain' (2021). <https://www.bsr.org/reports/BSR-Human-Rights-Due-Diligence-Products-Services.pdf>

- 90 Marisa McVey, 'Untangling the authority of external experts in the corporate implementation of the UN Guiding Principles on Business and Human Rights' (2022) *Journal of Human Rights*, 21, 5: 620–638.
- 91 Daniela Argento, Mashal Iqbal & Fitou Sonko, 'Challenges of sustainability-assurance practices: Insights from the Big 4 accounting firms'. In Jan Martin, Fredrik Nilsson & Peter Öhlman (eds) *Auditing Transformation* (2023) 250–272.
- 92 Theresia Harrer & Othmar M. Lehner, 'Assuring the unknowable: A reflection on the evolving landscape of sustainability assurance for financial auditors' (2024) *Current Opinion in Environmental Sustainability*, 67. <https://www.sciencedirect.com/science/article/pii/S1877343523001604>
- 93 Luc Fransen & Genevieve LeBaron, 'Big audit firms as regulatory intermediaries in transnational labor governance' (2019) *Regulation & Governance*, 13, 2. <https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12224>
- 94 Responsible Jewellery Council, 'What we do' (s.d.). <https://www.responsiblejewellery.com/>
- 95 IPIS, 'A tale of two diamond certification schemes: the Kimberley Process and the G7's Russian diamond ban' (2024). <https://ipisresearch.be/weekly-briefing/a-tale-of-two-diamond-certification-schemes-the-kimberley-process-and-the-g7s-russian-diamond-ban/>
- 96 Responsible Jewellery Council News, 'Alrosa steps down from the board of the Responsible Jewellery Council' (3 March 2022). <https://www.responsiblejewellery.com/alrosa-steps-down-from-the-board-of-the-responsible-jewellery-council-rjc/>
- 97 IRMA, 'First mine audited against world's most rigorous mining standard. Precedent-setting disclosure sets new bar for transparency' (21 October 2020). <https://responsiblemining.net/wp-content/uploads/2020/11/IRMA-Press-Release-First-Audit-21Oct2020.pdf>
- 98 For example, IRMA, 'Mine site assessment public summary report' (2020). <https://responsiblemining.net/wp-content/uploads/2020/10/Carrizal-Audit-Report-Public-Summary-Oct2020.pdf>
- 99 On the role of multi-stakeholder initiatives, see VENRO, Netzwerk für Unternehmensverantwortung and Forum Menschenrechte, 'Requirements for effective multi-stakeholder initiatives to strengthen corporate due diligence recommendations from the perspective of civil society' (s.d.). https://venro.org/fileadmin/user_upload/Dateien/Daten/Publikationen/Positionspapiere/MSI_Positionspapier_2020_Final_englisch.pdf
- 100 For a review of the academic literature, see Frank De Bakker, Andreas Rasche & Stefano Ponte, 'Multi-stakeholder initiatives on sustainability: A cross-disciplinary review and research agenda for business ethics'. (2019) *Business Ethics Quarterly*, 29, 3: 343–383.
- 101 The International Forum on Business Ethical Conduct, 'Global principles of business ethics for the aerospace and defense industry' (s.d.). <https://static1.squarespace.com/static/6268b8e1adda224613257ed2/t/626ae52b359672240ebfdc6f/1651172652779/IFBEC-Global-Principles.pdf>
- 102 Defense Industry Initiative on Business Ethics and Conduct, 'The DII principles' (s.d.). https://higherlogicdownload.s3.amazonaws.com/DII/03bf5a26-f29f-4c59-bee9-16be73aa4985/UploadedFiles/ZXJqEK2RTrWeDjdYotQA_DII%20principles.pdf
- 103 OECD, 'OECD due diligence guidance for responsible business conduct' (2018) 34. <https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf>
- 104 United Nations Human Rights Office of the High Commissioner, 'Guiding principles on business and human rights. Implementing the United Nations "Protect, Respect and Remedy" Framework' (2011) art. 22. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinessshr_en.pdf
- 105 OECD, 'OECD due diligence guidance for responsible business conduct' (2018) 32. <https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf>
- 106 Sarah Katz-Lavigne et al., 'Driving change in the Democratic Republic of Congo. An initial mapping of participation in mineral regulation and responsible sourcing' (University of Antwerp/IOB, April 2023) 62. <https://medialibrary.uantwerpen.be/files/8518/482b501d-4226-4b80-88fg-00d501fde4bd.pdf>
- 107 RMI, 'Downstream assessment program' (s.d.). <https://www.responsiblemineralsinitiative.org/responsible-minerals-assurance-process/downstream-program/>
- 108 SunStream, 'Know about the RMI's publish on downstream assessment program (DAP)' (s.d.). <https://www.sunstreamglobal.com/know-about-the-rmis-publish-on-downstream-assessment-program-dap/>
- 109 Human Rights Watch, 'Obsessed with audit tools, missing the goals: Why social audits can't fix labor rights abuses in global supply chains' (2022). https://www.hrw.org/sites/default/files/media_2022/11/Social_audits_brochure_1122_WEBSPREADS_0.pdf
- 110 Julianne Reineke & Jimmy Donaghey, 'Towards workerdriven supply chain governance: Developing decent work through democratic worker participation' (2021) *Journal of Supply Chain Management*, 57, 2. <https://ideas.repec.org/a/bla/jscmg/v57y2021i2p14-28.html>
- 111 BSR, 'Human rights due diligence of products and services assessing the downstream value chain'. (2021). <https://www.bsr.org/reports/BSR-Human-Rights-Due-Diligence-Products-Services.pdf>
- 112 Nick Bernards, Malcolm Campbell-Verduyn & Daivy Rodima-Taylor, 'The veil of transparency: Blockchain and sustainability governance in global supply chains' (2022) *Environment and Planning C: Politics and Space*, 23996544221142763.
- 113 Reshma Kamath, 'Food traceability on blockchain: Walmart's pork and mango pilots with IBM' (2018) *The Journal of the British*

Blockchain Association, 1, 1. [https://doi.org/10.31585/jbba-1-1-\(10\)2018](https://doi.org/10.31585/jbba-1-1-(10)2018)

- 114 IBM, 'Blockchain and sustainability through responsible sourcing' (28 December 2020). <https://www.ibm.com/blog/blockchain-and-sustainability-through-responsible-sourcing/>
- 115 Fairtrade Jewellery Co., 'Just Gold – fully traceable, conflict-free, artisanal gold from Democratic Republic of Congo – in partnership with an NGO' (s.d.). <https://ftjco.com/pages/just-gold-fully-traceable-conflict-free-artisanal-gold-from-democratic-republic-of-congo-in-partnership-with-an-ngo>
- 116 Nick Bernards, Malcolm Campbell-Verduyn & Daivy Rodima-Taylor, 'The veil of transparency: Blockchain and sustainability governance in global supply chains' (2022) *Environment and Planning C: Politics and Space*, 23996544221142763.
- 117 For example, SIPRI, 'Post-shipment on-site inspections: Multilateral steps for debating and enabling their adoption and use' (2022). https://www.sipri.org/sites/default/files/2022-10/sipripp63_post-shipment_onsite_inspections.pdf; SIPRI, 'Good practice guide on post-shipment on-site inspections of military materiel' (2022). https://www.sipri.org/sites/default/files/2022-08/sipri_2208_gpg_on-site_inspections.pdf.
- 118 Olivia Dean & Shelley Marshall, 'A race to the middle of the pack: An analysis of slavery and human trafficking statements submitted by Australian banks under the UK Modern Slavery Act' (2020) *Australian Journal of Human Rights*, 26, 1: 46–73. <https://doi.org/10.1080/1323238X.2020.1712515>
- 119 Danish Institute for Human Rights, 'Sustainability reporting and human rights. What can big data analysis tell us about corporate respect for human rights?' (2022). https://www.humanrights.dk/sites/humanrights.dk/files/media/document/DataAnalysis-CompanyReporting_EN_2022_accessible.pdf
- 120 Global Reporting Initiative, 'Corporate sustainability due diligence policies and sustainability reporting' (2023). https://www.globalreporting.org/media/cqho34tm/corporate_sustainability_due_diligence_and_sustainability_reporting_final.pdf
- 121 OECD, 'OECD due diligence guidance for responsible business conduct' (2018) 22–23. <https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf>
- 122 United Nations Human Rights Office of the High Commissioner, 'Guiding principles on business and human rights. Implementing the United Nations "Protect, Respect and Remedy" Framework' (2011) art. 16. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinessshr_en.pdf
- 123 World Benchmarking Alliance, 'Corporate human rights benchmark 2023: Insights report' (2023). https://assets.worldbenchmarkingalliance.org/app/uploads/2024/03/2023_Corporate_Human_Rights_Benchmark_-_Insights_Report_13Mar2024.pdf
- 124 Oxfam, 'Ripe for change: Ending human suffering in supermarket supply chains' (2018). https://oi-files-d8-prod.s3.eu-west-2.amazonaws.com/s3fs-public/file_attachments/cr-ripe-for-change-supermarket-supply-chains-210618-en.pdf
- 125 Lidl, 'Human rights in our supply chains: Progress update 2024' (2024). <https://corporate.lidl.be/fr/pdf/show/88491>
- 126 Ahold Delhaize, 'Human rights' (s.d.). <https://www.aholddelhaize.com/sustainability/our-position-on-societal-and-environmental-topics/human-rights/>
- 127 Hiruni Alwishewa, 'The move towards human rights due diligence policies by the arms industry' (Forum on the Arms Trade, 18 January 2024). <https://www.forumarmstrade.org/blog/the-move-towards-human-rights-due-diligence-policies-by-the-arms-industry>

**flemish
peaceinstitute**

www.flemishpeaceinstitute.eu

The Flemish Peace Institute is an independent institute dedicated
to peace research and hosted by the Flemish Parliament.