

GRID

**GUIDANCE FOR RESPONSIBLE INVESTMENT
IN DEFENCE-RELATED COMPANIES**

**LONDON CONSULTATION DRAFT
COMPANY EXPECTATIONS**

V0.1

12 JULY 2026

Contents

EXECUTIVE SUMMARY.....	3
INTRODUCTION.....	4
EXPECTATION 1 – AVOID LEGAL COMPLICITY.....	4
Policy.....	6
Risk management.....	6
Weapons Prohibited by Customary IHL	6
Weapons Prohibited by IHL Treaties	6
EXPECTATION 2 – RESPECT HUMAN RIGHTS.....	8
Policy.....	8
HRDD	9
HHRDD.....	9
Defence-Related Products or Services	10
Remedy	10
Stakeholder Engagement	10
EXPECTATION 3 – ELIMINATE BRIBERY AND CORRUPTION, INFLUENCE RESPONSIBLY AND BEHAVE ETHICALLY	11
Policies.....	11
Systems.....	12
SUPPORTING EXPECTATIONS	12
Contractual Controls and Counter Party Due Diligence	12
Awareness and Expertise	14
Transparency	14
ANNEX – DEFINITIONS AND BACKGROUND ON KEY TERMS AND ISSUES	14

EXECUTIVE SUMMARY

Overview – This draft chapter of the Guidance for Responsible Investment in Defence-related companies (GRID) sets out a set of expectations on defence-related companies. By meeting these expectations, companies will be well placed to address the legal, reputational, human rights and financial risks connected with the design, development, sale, export, use and misuse of their products or services.

The expectations are intended to be applicable to all defence-related companies, from large, listed corporations to early-stage private businesses, and relevant for companies involved in all products and services connected to defence (from missiles to microchips).

In summary, defence related companies are expected to:

1. Avoid legal complicity
2. Respect human rights
3. Eliminate bribery and corruption, influence responsibly and behave ethically

Under each of these expectations, more detail is set out concerning the policies and processes which companies should have in place. In addition, cross-cutting supporting expectations are set out concerning:

- Contractual controls
- Awareness and expertise
- Transparency

The expectations will shape the investor guidance, which will help investors understand how well aligned defence-related companies are to the expectations.

Note – This document is a draft version, created by the GRID Steering Group. Investors, defence-related companies and civil society organisations will all be consulted on the contents prior to a planned launch in Q4 2026. The Steering Group has approved this draft version for consultation, but it does not represent an agreed position of the organisations involved or their endorsement of the draft.

INTRODUCTION

Noting the huge range of business products and services connected to defence, this section focuses on cross cutting expectations for all defence related companies. It does not provide guidance for defence-related companies themselves, but it does set out further reading or examples of guidance and frameworks defence-related companies can explore.

Where possible, these expectations are explored in the Guidance. The GRID initiative and/or third parties may develop tools in the future to focus on specific scenarios or for types of defence related companies¹.

Companies which fail to meet the below expectations can create significant human rights, legal, reputational and financial risks and liabilities, which can translate into legal, reputational and financial risks for investors and financial institutions, and potentially create linkages between adverse human rights impacts and investors/financial institutions.

The Expectations are divided into four sections. The first three sections cover high-level expectations concerning *complicity in domestic and international crimes, the corporate responsibility to respect human rights, and the risks of bribery, corruption and unethical conduct*. These expectations are grounded in international laws and norms and should be read as pre-existing global expectations, not additional expectations created for GRID. The fourth section introduces several specific expectations which support the management of human rights, legal, reputational and financial risks across the previous three sections.

This draft chapter also includes a large annex covering definitions and background for key terms used throughout the document.

EXPECTATION 1 – AVOID LEGAL COMPLICITY

It goes without saying that companies should obey the law, and defence related companies must have robust compliance processes in place to navigate sanctions and domestic export control regimes. However, the GRID Steering Group believe that the potential civil and [criminal] legal liabilities relating to conflict and risks relating to International Law (especially International Criminal Law (ICL)) are underappreciated risks for defence related companies and so are expanded on in more detail.

Companies are expected to avoid complicity² in breaches of domestic or international law, which may occur where they are linked to gross human rights abuses or war crimes. Companies can

¹ See for example the UNIDIR proposed '[Framework of Responsible Industry Behaviour for AI in the Military Domain](#)'

² "ICL provides a [three-prong test](#) to determine complicity: (a) causation or contribution; (b) knowledge and foreseeability; and (c) proximity or remoteness. Causation determines whether a company's conduct enabled, exacerbated, or facilitated the gross human rights abuses and is equivalent to the concept of *actus reus* in criminal law. Knowledge and foreseeability, equivalent to the concept of *mens rea*, assess whether the business knew that its actions could *likely* contribute to gross human rights violations. Finally, proximity establishes whether the company was close – in terms of geography, duration, frequency, and intensity of interactions – to the principal perpetrator of the gross human rights

seek to avoid complicity by exercising heightened due diligence, using or developing leverage, and disengaging³ where serious violations cannot be prevented or mitigated. This expectation covers the business operations and value chains, including the design, development, sale, export, resale, use and disposal of their products and services. Integrating IHL and ICL into due diligence may also reduce the company's chances of legal accountability, for example by demonstrating that adequate steps were taken to know the risks and therefore negate the knowledge and foreseeability elements of complicity. Conversely, failure to conduct due diligence, despite the inherent risks from defence-related products and services, may increase the chance of a company entering a 'zone of legal risk'⁴. In other words, ignorance is no defence.

BREAK OUT BOX - Under ICL, corporate complicity risk arises where a company or investor:

- Knowingly provides practical assistance, support, or resources
- That have a substantial effect on the commission of an international crime
- And does so with knowledge of a real and foreseeable risk that its conduct contributes to that crime

Where these conditions are met (or increasingly foreseeable), continuing the business relationship can itself become legally problematic.

Disengagement may be an appropriate company approach to manage complicity risks.

***Note on ICL and Disengaging** – A person or company may incur liability if: they aid and abet breaches of international criminal law through the provision of practical assistance, encouragement or moral support; that has a substantial effect on the commission of an international crime; and where there is knowledge that assistance will contribute to the crime. Once those elements are met, continuing the relationship increases criminal exposure and disengagement may be the only effective way to stop 'practical assistance'. This reinforces the need for robust due diligence to avoid the connection to IHL or ICL breaches in the first place. The practical challenges concerning disengagement for companies are recognised. This challenge may be present for companies whose relationship with States is crucial for their business models and/or where there may be both long term contracts and legal consequences for breaking a contract. In addition, governments may cite national security interests and force companies to provide*

abuses.” [*The Role of Business in War: A Different Defense to Corporate Complicity? Part I: The Old Offense - Opinio Juris*](#)

³ Disengagement in this context is the decision by a company or investor to end, suspend, or materially withdraw from a business relationship (customer, client, supplier, joint venture, or investment) because continuing the relationship would risk contributing to, enabling, or being complicit in serious abuses, including war crimes, crimes against humanity, or other breaches of ICL.

⁴ [Vol.1-Corporate-legal-accountability-thematic-report-2008.pdf](#)

goods or services in line with however the government wishes to use them, whether or not that use is consistent with international law.

Policy - Defence related companies should express a clear commitment to supporting the principles of International Humanitarian Law⁵, the implementation of which is overseen at the most senior levels of the company.

Risk management - Defence related companies should implement comprehensive risk management systems. These systems should identify and manage complicity risks relating to their own business operations (including design, development, sale and export) as well as in the wider context of the use and misuse of their products and services, by exercising appropriate due diligence processes and employing such other levers as are necessary to guard against complicity risks. These processes are expected to be ongoing and to overlap with the Human Rights Due Diligence (HRDD) and heightened Human Rights Due Diligence (hHRDD) processes and are not expected to rely purely on export control measures. Due to the often long-term nature of defence contracting, due diligence prior to entering into a contract is vital.

Weapons Prohibited by Customary IHL⁶ – Companies domiciled in all jurisdictions should avoid involvement in the design, development, storage, sale or transport of weapons which are *prohibited by customary IHL* including: weapons of a nature to cause superfluous injury or unnecessary suffering ([see rule 70](#)); poisoned weapons ([see rule 72](#)); biological weapons ([see rule 73](#)); chemical weapons ([see rule 74](#)); expanding and exploding bullets ([see rule 77](#) and [78](#)); weapons primarily injuring by non-detectable fragments ([see rule 79](#)); and blinding laser weapons ([see rule 86](#)).

Weapons Prohibited by IHL Treaties⁷ – Companies should avoid involvement in the design, development, storage, sale or transport of weapons which are prohibited through the ratification of relevant IHL Treaties/Conventions by their state of domicile, or where such involvement would involve breaching additional IHL Treaties/Conventions ratified in countries where they operate or leave workers who are nationals of such countries in breach of relevant extra-territorial provisions. This may include the Convention on the Prohibition of Chemical Weapons (CWC), the Convention on the Prohibition of Biological Weapons (BWC), the Convention on Cluster Munitions (CCM), the Convention on the Prohibition of Anti-Personnel Mines (Ottawa Convention), and the Treaty on the Prohibition of Nuclear Weapons (TPNW).

Design and Development of Products and Service – Where companies are designing or developing new defence-related products or services, they are expected to determine whether its employment or foreseeable end uses would, in some or all circumstances, be

⁵ Consultation question – should the scope of this include ICL and IHRL?

⁶ The Guidance has used ICRC's International Humanitarian Law Databases as the authoritative source for [Customary IHL - Rules](#)

⁷⁷ The Guidance has taken the ICRC's IHL Databases as the source for [IHL Treaties - IHL Treaties](#)

prohibited by IHL, to inform their risk mitigation activities. Products and services should be ‘aligned by design’. For example, military digital command and control platforms should be developed to enable the lawful use of force and facilitate the integration of IHL aligned rules of engagement.

Parallel Project – Defence Tech and Responsible Investment

In October 2025, Heartland Initiative convened the Working Group on Defence Tech & Responsible Investment (“Working Group”) including institutional investors managing over \$16.5 trillion in assets and civil society experts at the vanguard of thought leadership on defence technologies. The Working Group is in the process of developing a “saliency-materiality” risk analysis framework, guidance for investor-led company engagement, and product- and conduct-based exclusionary screens. Focused on military AI, autonomous weapons systems, and high-risk surveillance, the guidance will be informed by a lawful-by-design approach throughout the life cycle of these technologies.

Further Reading: Companies and IHL - Red Cross Australia, plus RMIT University have produced a report detailing ‘Seven Indicators of Corporate Best Practice in International Humanitarian Law’⁸, which can help companies integrate IHL into their existing business and human rights frameworks.

Further Reading: Lawful Military AI – The issue of AI enabled decision support systems (AI-DSS) and Autonomous Weapon Systems as they relate to the design of Lawful Military AI (including a full lifecycle approach) is explored in the report by Zena Assaad and Jessica Dorsey⁹.

⁸ [7-indicators-of-corp-best-prac-final-2021.pdf](#)

⁹ [Designing Lawful Military AI: Technical and Legal Reflections on Decision-Support and Autonomous Weapon Systems](#) - Perry World House

EXPECTATION 2 – RESPECT HUMAN RIGHTS

All companies have a responsibility to respect human rights as articulated in international standards on business and human rights. Respect for human rights means that companies should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved. Companies which provide defence related products or services to governments or militaries can be connected to adverse human rights impacts which involve their products or services. This is true even where the end user is separated from the company by many supply chain or transfer layers. The UNGPs provide a framework for understanding that linkage and the company responsibilities to prevent, avoid, mitigate and remediate those human rights impacts.

The international standards on business and human rights are increasingly being translated into domestic and supranational legislation which place legal duties on companies. They are also increasingly being invoked in civil and criminal proceedings to e.g. interpret standards of care, assess corporate conduct, fill normative gaps where binding law is general or unspecified and to evaluate due diligence expectations¹⁰.

Defence related companies should conduct due diligence to avoid infringing on the rights of others and address adverse impacts with which they are involved, through their products, services or business relationships¹¹. They should implement responsible business conduct practices as detailed in [International standards on business and human rights](#). These expectations exist in the absence of mandatory due diligence legislation, or where due diligence legislation only focuses on parts of the value chain. For defence companies, due diligence also reflects important mitigation of the company's material legal and therefore financial risks.

This section is provided to give a high-level explanation of defence-related company human rights responsibilities under the UN Guiding Principles on Business and Human Rights (UNGPs). The UNGPs do not replace IHL or IHRL, they translate state-centric international human rights standards into corporate responsibilities. In situations of armed conflict, companies are expected to respect the standards of IHL, in addition to IHRL. The subsections below set out expectations concerning company policy, HRDD, hHRDD, access to remedy and stakeholder engagement¹².

Policy – Companies should enshrine their commitment to respect human rights in an organisational level policy document approved at the most senior level. The commitment should cover the respect for all internationally recognised human rights across the company's own activities and value chain. For defence companies, this includes foreseeable end uses by indirect customers of the company.

¹⁰ Consultation Note - The plan is to add examples / case studies to flesh out the context

¹¹ This includes operations and supply chain, but a core focus for GRID is the downstream use and potential misuse of defence related products and services

¹² There is a significant body of work which already explains what these expectations mean in practice and the GRID will only provide a high-level overview, supported by key references and further reading.

HRDD – Companies should implement robust human rights due diligence (HRDD) processes commensurate with the risk of the company or its products and/or services causing, contributing, or being directly linked to adverse human rights impacts, including involvement in IHL breaches. HRDD processes should:

- Identify and assess actual and potential human rights impacts
- Integrate the findings of assessments and take action to prevent or mitigate potential impacts, prioritising the most salient human rights risks and impacts
- Track and measure the company performance
- Communicate their progress and performance

Meeting host nation licenses and export control regime requirements can help mitigate human rights related risks. But licenses, accreditations, or export via government mandated foreign military sales programmes are not sufficiently robust to be a replacement for HRDD. Companies should not rely exclusively on licensing or export regimes. At the same time, HRDD can bridge differences across different export regimes, enabling a consistent approach which is controlled by the company, not outsourced to a third party.

Further Reading: Industry Guidance – The American Bar Association’s Center for Human Rights published ‘[Defence Industry Human Rights Due Diligence Guidance](#)’ in 2022. This does not cover policy language but neatly brings the legal and human rights due diligence elements into one framework which, if fully implemented, would go a long way to meeting the due diligence expectations set out in this chapter. While focused on the Arms Industry, this guidance is relevant to all defence related companies, including in the tech industry. The table below sets out the key elements of the Guidance.

HHRDD – Certain contexts, such as international armed conflict, non-international armed conflict, occupation and situations with widespread violence increase the likelihood of severe adverse human rights impacts. Where companies are connected via operations or business relationships to ‘Conflict Affected and High-Risk Areas’ (or CAHRAs), they should implement *heightened* human rights due diligence (hHRDD¹³). In short this means building on HRDD to undertake sufficient analysis of the conflict and the actions of the parties to identify and assess actual or potential adverse impact on conflict that the company may cause or contribute to through its own activities, or that it may be directly linked to via its operations, products or services, in the particular context of the conflict.

¹³ [UNDP Heightened Human Rights Due Diligence for Business in Conflict-Affected Context.pdf](#) and [Investor Toolkit on Human Rights and Armed Conflict - Toolkits](#). There is no singular list of all CAHRAs in the world and any list would be dynamic; adjusting as conditions on the ground change.

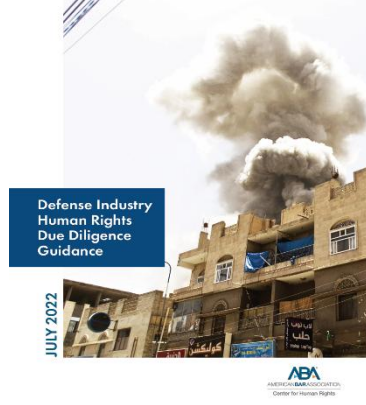
Defence-Related Products or Services

Selling Defence-related products and services to military customers in an area that is or becomes a CAHRA is likely to have the implications that arise in HHRD from “contributing to” any human rights abuses committed with those products or services. These generally include the need to cease any further contribution and to contribute to remedy for the victims. HHRDD would additionally require a pro-active understanding of the military customers use of the products or service and how they may contribute to the conflict. As an example, this may require defence companies to consider flash- or trigger points that could result in human rights violations.

Further Reading: Industry Guidance – The Australian Red Cross and the Royal Melbourne Institute of Technology are producing Guidance for Business on how to integrate IHL into HHRDD, which will be published in 2026. They are supporting this with a one-day training course for relevant company staff.

Remedy – Companies should develop and implement adequate processes to provide or enable remedy for impacted people where the company has caused or contributed to an adverse human rights impact¹⁴.

Stakeholder Engagement - Stakeholder engagement is a key step for meeting the policy, due diligence and remedy expectations above. In line with the UNGPs, defence-related companies should explore appropriate stakeholder engagement.¹⁵

American Bar Association – Industry Guidance ¹⁶	
Overview of ABA Guidance Consistent with OECD standards, it models a risk-based approach to due diligence ⁶⁸ encompassing four unique stages: risk assessment, prevention and mitigation, end-use monitoring, and investigation and remediation. This action plan should be incorporated by exporters into a policy that is approved at the most senior level, incorporated throughout its business operations, and overseen by a dedicated compliance unit.	
Elements of Due Diligence	
: a. Stage 1: Risk Assessment i. Contextual Risk Assessment	c. Stage 3: End-Use Monitoring i. Client Reporting Obligations ii. Audits and Site Inspections

¹⁴ To discuss the practicalities of this in the consultation, as well as the ability to include examples in practice, e.g. Saab.

¹⁵ TBC how much detail is required on Stakeholder Engagement

¹⁶ [Defense Industry Human Rights Due Diligence Guidance](#)

ii. Client Risk Assessment iii. Regulatory Authority Reliability Assessment	iii. Open-Source Information Collection and Stakeholder Engagement
b. Stage 2: Prevention and Mitigation Measures i. Build Prevention and Mitigation into Business Contracts ii. Training iii. Establish a Red-Flag System iv. Industry-Level Collaboration	d. Stage 4: Investigation and Remediation i. Internal Investigation of Potential Misuse ii. Contractual Penalties iii. Policy and Operations Review and Remediation iv. Cooperation in External Investigations and Fact-Finding

EXPECTATION 3 – ELIMINATE BRIBERY AND CORRUPTION, INFLUENCE RESPONSIBLY AND BEHAVE ETHICALLY

Defence related companies are expected to operate to high ethical standards, and we recognise the efforts of industry bodies such as IFBEC to create the Global Principles of Business Ethics for the Aerospace and Defence Industry¹⁷.

Noting the heightened risks relating to bribery and corruption and improper advantages in the defence sector, all defence-related companies should have robust policies and systems in place to manage these risks¹⁸.



Political advocacy and lobbying should be transparent and aligned with human rights and anti-bribery and corruption commitments and should avoid undue influence on export decision-making or licensing. It should also be aligned with internal complicity and human rights risk assessments, so that companies do not advocate for the export of products to, or use of services by, governments who are assessed to be at a high risk of abusing human rights or breaching international law¹⁹.

Policies – Defence related companies should commit to the prohibition and elimination of all forms of bribery and corruption in their business operations and business relationships and should prohibit conduct which involves improper advantages²⁰. This

¹⁷ IFBEC is the International forum on Business Ethical Conduct for the global aerospace and defence sector. See [IFBEC](#)

¹⁸ To add reference to the UN Convention against Corruption, OECD Anti-Bribery Convention, UK and other extra-territorial legislations

¹⁹ Companies will have their own approaches to understanding sovereign risks, but sources such as Transparency International's Corruption Perception Index, Freedom House's Freedom Scores and sanctions list can provide useful starting points.

²⁰ Improper advantages concern using the offer, promise or provision of undue pecuniary or other advantages (e.g. payments, gifts, hospitality, as well as political contributions or charitable

should be formalised in a policy that is approved and overseen at the highest level of the company. These commitments should apply to all business partners and across all jurisdictions, regardless of local laws or legal enforcement.

Systems – Companies should implement robust, demonstrable, risk-based, anti-bribery and corruption management processes to deliver on their policy commitments²¹. These systems should align with the OECD Guidelines ([Chapter VII](#)) and should protect whistleblowers from retaliation²². Companies should also implement systems to manage improper advantage risks, including the tracking and monitoring of payments, gifts, hospitality, political or charitable donations, and engagements with political actors, partners, advisors and intermediaries. Advisers, agents and intermediaries should be subject to particularly careful and on-going due diligence.

Ethical conduct should also preclude the use of strategies to circumvent export controls or sanctions through e.g. the use of off-shore entities or third parties.

SUPPORTING EXPECTATIONS

The additional expectations below support the management of human rights, legal, reputational and financial risks for defence-related companies and frequently support 1-3 above:

Contractual Controls and Counter Party Due Diligence – As part of the complicity and human rights due diligence, defence-related companies should conduct detailed pre-contractual due diligence on the sale, or purchase, of products or services to/from third parties followed by regular reviews to avoid or mitigate human rights, legal, reputational and financial risks and potential risks, covering at a minimum:

- The extent of any legal licensing requirements [and sanctions]
- The risk profile of the direct customer / client / intermediary, including historical transactions, length of relationship and previous controversies involving the counterparty
- The risk profile of the country of destination, including its involvement in armed conflict or military occupation, levels of authoritarianism, and levels of public sector corruption
- Intended and likely end use of the specific products or services
- Intended and likely end user of the specific products or services
- Diversion risks for products or services

donations), to public officials, political parties or political candidates, or to any private party, in order to obtain or retain business or gain any other improper advantage in the conduct of their business).

[07_4PGlobalPrinciples_A4.indd](#)

²¹ Companies may already be compliant with national anti-bribery and corruption laws including the UK Bribery Act 2010 which provide a defence for companies with adequate procedures in place to prevent associated persons from bribing. Such procedures are likely to meet these expectations, provided they are fully implemented in each case and not treated as a box-ticking exercise.

²² The IFBEC (International Forum on Business Ethical Conduct for the Aerospace and Defence Industry) have developed a set of [Global Principles](#) of Business Ethics which companies voluntarily implement.

- Any ongoing support or maintenance relationships
- The current and potential leverage of the company with its clients, customers or end users²³
- Intended or foreseeable disposal or decommissioning of products or services

Where there is a clear risk that the products or services might enable or facilitate serious human rights violations or breaches of IHL and such risks cannot be mitigated, companies are expected to refrain from proceeding with the sale or service provision.

BREAK OUT BOX e.g. Itochu Corporation²⁴ reportedly cancelled an MoU with a defence contractor, even though the MoU was made at the request of Japan's Defence Ministry, resulting in the suspension of imports from a company alleged to be involved in breaches of international law.

Companies are expected to explore mitigating actions proportionate to the risks including:

- Training internal staff, executives and board members on relevant risks and company systems. This is particularly relevant where there are competing priorities within a company (e.g. where executives or sales teams are incentivised to act in ways unaligned with company commitments).
- The inclusion of strict end-use, resale, transparency and auditing clauses, as well as the right to suspend or terminate contracts or services if evidence emerges of misuse or diversion, in contracts²⁵.
- Integrating risk aggregators, human rights red flags, and other types of open-source intelligence into KYC due diligence, moving beyond a “compliance only” framework.
- Ensure that a “lawful-by-design” approach is integrated at each stage of the product life cycle, from R&D to end use²⁶.
- Maintaining through life monitoring and investigation of potential misuse and contractual breaches and ensuring information feeds back into decision making such as contract renewal, provision of spare parts or ongoing maintenance and support services.
- Training staff in the lawful use of equipment or services.
- Training clients in lawful use of equipment or services, where relevant.
- Prohibiting the use of strategies to circumvent export controls or sanctions through e.g. the use of off-shore entities or third parties.

²³ To consider adding further requirements concerning business partner relationships

²⁴ [Human Rights Due Diligence Within the Arms Industry: Challenges, Practices and Opportunities | Business and Human Rights Journal | Cambridge Core](#)

²⁵ To consider the creation of model / example contract template clauses

²⁶ A useful reference - [Designing Lawful Military AI: Technical and Legal Reflections on Decision-Support and Autonomous Weapon Systems - Perry World House](#)

Awareness and Expertise - Defence related companies should develop and maintain appropriate levels of knowledge on international criminal law, international humanitarian law, and civil and criminal liability, across the various jurisdictions relevant to their operations and the end-use of their products or services. They should also develop in house expertise on the implementation of international business and human rights standards and, where appropriate, seek external expertise to support the development and implementation of policies and processes. Where awareness and expertise most appropriately sit will depend on the specific context of the company, but Board members should always have awareness.

Transparency – Defence related companies are expected to be as transparent as possible without causing *genuine* security risks, so that investors can understand the presence and severity of human rights, legal, reputational, and financial risks. Transparency does not necessarily imply public disclosures (e.g. for early-stage companies). Disclosures of policies, processes and performance will provide some level of reassurance to investors where confidentiality precludes disclosing more specific information.

ANNEX – DEFINITIONS AND BACKGROUND ON KEY TERMS AND ISSUES

Internationally recognized human rights.²⁷ As noted in the UN Guiding Principles on Business and Human Rights, the responsibility of business enterprises to respect human rights refers to internationally recognized human rights, which are understood, at a minimum, as being those expressed in the [Universal Declaration of Human Rights \(UDHR\)](#), the [International Covenant on Civil and Political Rights](#), the [International Covenant on Economic, Social and Cultural Rights](#), and the principles concerning fundamental rights set out in the [ILO Declaration on Fundamental Principles and Rights at Work](#), which can be referred to as International Human Rights Standards. Depending on circumstances, business enterprises may need to consider additional standards, such as those found in [other human rights instruments](#) and in [international humanitarian law](#).

International human rights law (IHRL) lays down obligations which States are bound to respect. By becoming parties to international treaties, States assume obligations and duties under international law to respect, to protect and to fulfil human rights. The obligation to respect means that States must refrain from interfering with or curtailing the enjoyment of human rights. The obligation to protect requires States to protect individuals and groups against human rights abuses. The obligation to fulfil means that States must take positive action to facilitate the enjoyment of basic human rights²⁸.

Adverse human rights impact. An adverse human rights impact occurs when an action or omission removes or reduces the ability of an individual or community to enjoy their human rights.

²⁷ ([Access to Remedy in Cases of Business-Related Human Rights Abuse](#))

²⁸ [International Human Rights Law | OHCHR](#)

Adverse human rights impacts in conflict. ‘Lex specialis’ is a term often used when describing the relationship between IHRL and IHL. IHL is designed specifically for situations of armed conflict and while it does not cancel out IHRL, it in effect overrides elements of it. For example, the right to life is non-derogable and the International Covenant on Civil and Political Rights (ICCPR), Article 6, states ‘No one shall be arbitrarily deprived of his life’. IHRL bans arbitrary killings, while IHL determines what is arbitrary in the context of conflict. IHL regulates acceptable activity within conflict such that specific military actions conducted in line with IHL do not equate to a breach of IHRL²⁹.

An adverse human rights impact in conflict will often relate to action that does not align with IHL. In the bluntest terms, for the sake of the UNGPs deaths in conflict do not necessarily equate to an adverse human rights impact. Note that this relates to conduct within conflict – there are other ways companies can cause, contribute or be linked to adverse human rights impacts which are not directly correlated to a human rights violation, such as making conflict itself more likely to happen.

Human rights abuse. The term “human rights abuse” refers to actions or omissions which may result in or amount to a breach of international human rights. There is a considerable overlap between the term “human rights abuse” and “adverse human rights impact” although the latter, which is defined by reference to degrees of enjoyment of human rights, has a broader scope. There is also a considerable degree of overlap between the concepts of human rights abuse and human rights violation (defined below). In the Guiding Principles, the term “human rights abuse” is used to refer to abuses committed by non-State actors, including business enterprises.

Human rights violation. A human rights violation is a violation of an obligation under **international human rights law**. Under international law, the primary addressees and ultimate guarantors of human rights are States. Thus, a reference to a human rights violation (as opposed to human rights abuse, defined above) will almost always refer to a breach of international human rights law by a State. States become subject to international human rights obligations in various ways, including through customary international law, and by virtue of their treaty commitments.

International business and human rights standards (BHR standards). There are multiple international standards on business and human rights (BHR standards) which cover different aspects of business and their interaction with human rights, international human rights law and international humanitarian law. The four BHR standards set out below are the most widely recognised:

- The UN Guiding Principles on Business and Human Rights ([UNGPs](#)) were unanimously endorsed by the UN Human Rights Council in 2011 and constitute the global standard for preventing and addressing the risk of adverse impacts on human rights involving business activity. The UNGPs cover the state duty to protect human rights, the corporate responsibility to respect human rights and the access to remedy (to counteract or make good any human rights harms). The UNGPs apply to all States and to all enterprises, both multinational and others, regardless of their size, sector, operational context, ownership and structure.

²⁹ This issue will be explored in the consultation phases to discuss the interplay between IHRL violations, conflict and e.g. International Crimes.

- The ILO Tripartite Declaration of Principles concerning Multinational Enterprises and Social Policy ([MNE Declaration](#)), which aims to encourage MNEs to contribute to economic and social progress, help realise decent work for all and minimise and resolve difficulties related to MNE operations. The MNE Declaration is aligned with the UNGPs.
- The OECD Guidelines for Multinational Enterprises ([OECD Guidelines](#)), which provide recommendations addressed by governments to MNEs operating in, or from, the territories of adhering countries, wherever they operate, while taking into account the particular circumstances of each host country. They provide non-binding principles and standards for responsible business conduct in a global context consistent with applicable laws and internationally recognised standards. The OECD Guidelines' chapter on Human Rights is aligned with the UNGPs and the chapter on Employment and Industrial Relations is aligned with ILO Tripartite Declaration.
- The Ten Principles of the UN Global Compact ([UNGC](#)), which cover responsible business conduct expectations across human rights, labour, environmental and anti-corruption areas, and which are derived from several core human rights declarations and conventions (the UDHR, the ILO Declaration on Fundamental Principles and Rights at Work, the Rio Declaration on Environment and Development, and the UN Convention Against Corruption).

All the BHR standards detailed above are complementary, mutually reinforcing, and aligned with underlying internationally recognised human rights and form a comprehensive framework³⁰.

The ILO MNE Declaration and the OECD Guidelines both explicitly reference the UNGPs and can be considered aligned standards while having different material scopes. The Principles for Responsible Contracts, considered as an addendum to the UNGPs,³¹ deals with a different subject matter, and has therefore not been included here.

The UNGC 10 Principles predate the other four standards. Principle 1 requires participating businesses to support and respect the protection of internationally proclaimed human rights, and Principle 2 requires businesses to ensure that they are not complicit in human rights abuses. The UNGC, as an organisation, has recognised that the UNGPs are a global standard applicable to all business enterprises and provide an authoritative framework for UNGC participants on the policies and processes they should implement in order to ensure they meet their responsibilities under Principles 1 and 2 of the UNGC³².

Human rights due diligence (HRDD) – Human rights due diligence is the ongoing process by which a company identifies, prevents, mitigates, and accounts for how it impacts people's human rights through its own activities and its business relationships. It is a continuous risk-management process focused on risks to people, not risk to the organisation. HRDD is anchored in the UNGPs, meaning that all companies, regardless of size, sector or location, are expected to identify, prevent and mitigate human rights risks and impact, track the effectiveness of their actions and communicate their efforts and progress.

³⁰ See [Brochure-responsible-business-key-messages-from-international-instruments-ENG](#)

³¹ [The Principles for Responsible Contracts](#), which provide 10 key principles to help integrate the management of human rights risks into contract negotiations between States and foreign business investors.

³² See the joint note between the UN Global Compact and the UN OHCHR from 2011 [issues_doc/human_rights/Resources/GPs_GC+note.pdf](#)

Heightened human rights due diligence (HHRDD) – The UNGPs envisioned HRDD processes being proportionate to the risk, with heightened risk contexts resulting in ‘heightened human rights due diligence’. Conflict Affected and High-Risk Areas (CAHRAs) generate elevated risks of human rights abuses. Where companies are operating in or connected to CAHRAs they should therefore be conducting HHRDD. HHRDD is not just ‘more due diligence’. “Heightened human rights due diligence strengthens the understanding of the context where businesses operate and ensures that their activities do not contribute to violence by identifying flash points, potential triggers or the forces that are driving the conflict”.³³

Remediation/remedy. The terms “remediation” and “remedy” are often used interchangeably. These terms respectively refer to the processes of providing remedy for an adverse human rights impact, or the substantive outcomes that can counteract or make good the adverse impact. These outcomes may take a range of forms, such as apologies, restitution, rehabilitation, financial or non-financial compensation, or punitive sanctions (whether criminal or administrative, such as fines), as well as the prevention of harm through injunctions or other guarantees of non-repetition, for example. An effective remedy should be a remedy to the victim(s) and not, for example, a fine paid to the State.

Value chain. A value chain of a business enterprise refers to the activities, operations and business relationships relevant to the production, supply and distribution of products and/or the provision of services by that business enterprise, both upstream and downstream. Within a value chain:

- Upstream business relationships include those concerned with the supply of goods or services relevant to the operations of the company or the development, production or supply of the company’s own products or services, whereas
- Downstream business relationships include those relevant to the distribution, use or consumption of the business enterprise’s products or services, and may extend to the entities involved in the disposal of products.

Business relationship. According to the OECD MNE Guidelines, the term ‘business relationship’ includes relationships with business partners, sub-contractors, franchisees, investee companies, clients, and joint venture partners, entities in the supply chain which supply products or services that contribute to the enterprise’s own operations, products or services or which receive, license, buy or use products or services from the enterprise, and any other non-State or State entities directly linked to its operations, products or services. Relationships with individual consumers, who are natural persons acting for purposes that are unrelated to a business, commercial, or governmental activity, are not generally considered ‘business relationships’ although an enterprise can contribute to adverse impacts caused by them. Business relationships include relationships beyond contractual, first tier or immediate relationships.

IHRL AND IHL

³³ [Heightened Human Rights Due Diligence for Business in Conflict-Affected Contexts: A Guide | United Nations Development Programme](#)

This section has been reproduced with permission from the Human Rights Working Group, 2023, "Investor Toolkit on Human Rights and Armed Conflict", Responsible Investment Association Australasia, [Investor Toolkit on Human Rights and Armed Conflict - Toolkits](#)

“International human rights law

International human rights law (IHRL) is a set of international rules, established by treaty and custom, on the basis of which individuals and groups can expect and claim certain rights that must be respected and protected by States. International human rights standards also contain numerous non-treaty-based principles and guidelines ('soft law'). The International Committee of the Red Cross (ICRC) has a useful explanation of the differences and similarities between IHL and IHRL.³⁴

The core principles of IHRL are enshrined in the Universal Declaration of Human Rights (UDHR), and the fundamental rights incorporated in the UDHR are codified in the two universal instruments:

- International Covenant on Civil and Political Rights (ICCPR); and
- International Covenant on Economic, Social and Cultural Rights (ICESCR)

Together these three instruments form what is known as the International Bill of Rights.

A series of subsequent international human rights instruments have expanded the body of international human rights law, such as the Convention on the Elimination of All Forms of Discrimination against Women (1979) and the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (1984). In total, there are nine core international human rights instruments, each of which has a committee of experts to monitor implementation of the treaty provisions by its States' parties. There are also regional instruments such as:

- European Convention on Human Rights (1950)
- American Convention on Human Rights (1969)
- African Charter on Human and Peoples' Rights (1981)

International humanitarian law

International humanitarian law (IHL) is also known as 'the law of armed conflict' or 'the law of war'. Its fundamental premise is that even in times of armed conflict human dignity must be respected and protected, and the means and methods of warfare regulated. Rules reflecting these principles can be found throughout history in most if not all cultures. The law of armed conflict is based on customs and traditions and our experience of armed conflict throughout the ages. A good example is the universal ban on poisoning as a form of warfare, which dates to ancient times when, for example, the military on both sides would issue orders not to poison

³⁴ ICRC (2015) <https://www.icrc.org/en/document/what-difference-between-ihl-and-human-rights-law>

wells, as much for their benefit as for that of the civilian population – they might need the water one day.

Over the years, these customs, traditions and experiences have developed into ‘hard law’, namely treaty law and customary international humanitarian law. Both are legally binding and together comprise the key sources of modern IHL. In short:

- **The four Geneva Conventions of 1949 and their Additional Protocols form the fundamental core of IHL treaty law.** These are complemented by a series of other legally binding instruments, often designed to regulate specific means or methods of warfare, such as the use of certain weapons.
- **Customary IHL** consists of rules that arise out of repeated and consistent practice in armed conflict by States that, as a result, become accepted and recognised as universally binding law. Customary IHL exists independent of treaty law but also complements and strengthens it.

At its core, IHL lays out the protections for those who are not or are no longer taking part in the fighting – civilians, prisoners of war, injured soldiers, medical personnel etc. – as well as civilian objects, property, and the environment. IHL also dictates which weapons and military tactics can be used by parties to an armed conflict and how, what objects can be lawfully targeted, and which acts may amount to war crimes. For business, IHL helps to clarify which actions are considered ‘closely linked to an armed conflict’. In many ways, ‘responsible’, and even ‘legal’, conduct in armed conflict may hinge on whether and how a business is directly or indirectly linked to that conflict or its parties. It is also important for businesses operating in a conflict-affected context to understand which actions could result in a company, its personnel or its assets losing the protections of civilian status under IHL. Take, for example, a telecommunications company that procures and provides intelligence to a party to an armed conflict, which results in a military strike against another party, or even disrupts.

This will amount to ‘direct participation in hostilities’ and would result in the company losing civilian immunity under IHL.³⁵ Unlike the law governing the use of force by one State against another (jus ad bellum) – set out in the UN Charter – IHL is not concerned with the legality of war or the act of going to war. Rather, as long as an armed conflict exists, IHL will apply to any activity related to that conflict. Similarly, as IHL only applies in the context of armed conflict, other legal frameworks (including international human rights law, see below) exist to govern conduct in peacetime or in a period of violence that fails to meet the threshold of armed conflict under IHL. Situations such as these may require authorities to deploy specialist law enforcement, such as riot police, or even the armed forces to restore peace and order – but this will not automatically invoke the application of IHL. Rather, domestic law, including human rights law and national criminal law, will continue to apply. In some cases, these laws act concurrently with IHL. For example, human rights law doesn’t simply cease to exist in situations of armed conflict, rather there is considerable overlap but also significant differences.

³⁵ 59 OpinioJuris (2022) <https://opiniojuris.org/2022/09/12/military-information-sharing-by-ukrainian-citizens-in-the-digital-environment-dph-blurring-of-lines-between-civilian-and-military-actors-in-ukraine/>

IHL and IHRL: how are they linked?

IHL is distinct from IHRL but also inextricably linked for business and investors.

International humanitarian law and international human rights are complementary bodies of law that simultaneously apply in times of war. Both share certain common goals, such as the protection of life, health, dignity and property. Because international humanitarian law is more specifically focused on the regulation of armed conflict, in such contexts human rights will often be interpreted based on standards of international humanitarian law³⁶.

To reiterate, IHL is the specialist body of law that applies exclusively to situations of armed conflict and military occupation. Therein lies one of the key differences between these legal frameworks. IHL is intended to prevent and respond to humanitarian problems that arise during war and contains rules that deal with issues that are not found in human rights law, such as the conduct of hostilities, prisoner of war status and the protection of civilian people and infrastructure. Unlike IHL, international human rights law applies at all times – in peace and in war – and sets standards for States' treatment of individual and collective rights and freedoms.

Human rights are inherent entitlements that belong to every person because they are human. There are certain critical human rights that must never be derogated from, such as the right to not be tortured. However, it is possible for some human rights to be suspended in certain situations of public emergency, such as armed conflict. Such derogation is not permitted under IHL, as these laws were designed for that very emergency. In addition to this difference in the temporal scope of application, IHL and IHRL also differ in their geographical scope of application.

It is accepted that IHL applies extraterritorially, as it was borne of a need to regulate the conduct of State(s) involved in conflict on the territory of another and, similarly, in the context of non-international armed conflicts when that conflict crosses territorial borders. It is widely accepted that IHRL also applies extraterritorially, for example when a State occupies and exercises control over another territory, but the extent to which it does in other contexts is yet to be determined. For example, in the application of human rights norms in extraterritorial lethal-force operations, such as counterterrorism operations, that take place in non-conflict contexts.

Another fundamental distinction between these legal frameworks is that IHRL is traditionally only binding on governments (**noting though that many IHRL principles are incorporated into domestic laws, creating criminal and civil liabilities for companies**) – it governs the relationship between a State and individuals/groups on its territory and under its jurisdiction. However, IHL binds all parties to an armed conflict – States and non-State armed groups – as well as other non-State actors. This can include legal persons, such as companies, as well as individual personnel and executives of businesses whose activities are closely linked to an armed conflict³⁷.

In summary, the outbreak of armed conflict (and therefore the application of IHL) introduces rules and protections that will either complement, supplement or conflict with, and possibly prevail

³⁶ ICRC (2006) <https://www.icrc.org/en/doc/resources/documents/misc/business-ihl-150806.htm>

³⁷ [Private Businesses and Armed Conflict: An Introduction to Relevant Rules of International Humanitarian Law | International Committee of the Red Cross](#)

over, human rights laws in that territory, potentially increasing risk and exposure for companies and investors. For example, IHRL dictates that any deprivation of life must not be arbitrary. In such cases, IHL can help to define arbitrariness in the context of an armed conflict, i.e. the use of lethal force between warring parties.

The risk of companies becoming involved in grave human rights abuses is particularly high in contexts affected by armed conflicts and other situations of widespread violence. These situations differ widely, involving state and non-state actors (such as armies or guerrilla groups), varying ambitions (such as obtaining territory or resources) and underlying motivations (such as imposing an ideology or gaining a profit)³⁸.

³⁸ UNDP (2022) Heightened Human Rights Due Diligence for business in conflict-affected contexts: A Guide, <https://www.undp.org/publications/heightened-human-rights-due-diligence-business-conflict-affected-contexts-guide>



Figure 1 - Draft explanation of interplay between IHL, IHRL, UNGPs

International Criminal Law (ICL)

“ICL covers the gravest crimes recognised by the international community: genocide, crimes against humanity, war crimes, and, in some jurisdictions, the crime of aggression. These are codified primarily in the Rome Statute of the International Criminal Court (ICC) (Articles 6–8) and implemented into domestic legal systems across the world”.³⁹

[Blind Spot in the Boardroom, GBI Issue Paper, Gerald Pachoud, February 2026](#)

Complicity

“Corporate complicity is a complex issue that is used by different people in different ways. The UNGPs state the following: “Questions of complicity may arise when a business enterprise contributes to, or is seen as contributing to, adverse human rights impacts caused by other parties. Complicity has both non-legal and legal meanings. As a non-legal matter, business enterprises may be perceived as being ‘complicit’ in the acts of another party where, for example, they are seen to benefit from an abuse committed by that party.”

The UN Global Compact (UNGC) states that “Complicity means being implicated in a human rights abuse that another company, government, individual or other group is causing” based on an act or omission by a company that helps another in some way to carry out a human rights abuse, and the knowledge by the company that its act or omission could provide such help. UNGC Principle 2 states companies should make sure they are not complicit in human rights abuses.”

[Guidance for ESG Data Providers, Investor Initiative on Human Rights Data, September 2025](#)

*For the purpose of this guidance, complicity discussions will focus on **LEGAL COMPLICITY** (see section below).*

LEGAL COMPLICITY AND LIABILITY FOR DEFENCE RELATED COMPANIES

*“As a legal matter, most national jurisdictions prohibit complicity in the commission of a crime, and a number allow for criminal liability of business enterprises in such cases. Typically, civil actions can also be based on an enterprise’s alleged contribution to a harm, although these may not be framed in human rights terms. The weight of international criminal law jurisprudence indicates that the **relevant standard for aiding and abetting is knowingly providing practical assistance or encouragement that has a substantial effect on the commission of a crime**”.*

[Principle 17, UNGPs, 2011](#)

Extraterritorial and domestic law creates legal complicity risks for companies, their directors and staff. Noting the heightened risks of human rights violations in conflict affected and high-risk areas, as well as the linkage between the products and services of defence related companies

³⁹ Rome Statute of the International Criminal Court (2002), available at: <https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf>

and potential violations, *legal complicity* in breaches of ICL, IHL, IHRL and their domestic translations, and *civil and legal liability*, are significant risks for companies.

Gerald Pachoud provides a succinct explanation in the Feb 2026 GBI Issue Paper⁴⁰:

“Criminal responsibility may arise where a person knowingly provides assistance that has a meaningful effect on the commission of international crimes. This assistance may take many forms, including financing, logistical support, the provision of goods or services, or operational facilitation... In plain terms: if you knowingly provide meaningful support that makes it easier for others to commit atrocities, you can be criminally liable.”

The following section has been reproduced from the GBI Issue Paper to provide additional context during the consultation process:

“Assistance (“Actus Reus”) - The assistance must be practical (e.g., providing goods, financing, logistics) or moral (e.g., encouraging or legitimising perpetrators). It can include:

- Providing weapons or equipment later used in unlawful attacks.*
- Financing or otherwise materially supporting an armed group or state entity committing atrocities.*
- Supplying infrastructure or services (e.g., transport, communications, energy) that enable or facilitate crimes.*
- Offering strategic advice or technical expertise knowing how it will be used.*

The threshold: The assistance must have a “substantial effect” on the commission of the crime.⁴¹ This does not mean the crime would not have happened without it, but that the assistance made a significant difference.

Knowledge or purpose (“Mens Rea”) - The mental element for aiding and abetting under ICL has long been debated, but international jurisprudence has gradually clarified the boundaries of responsibility.⁴² Early case law from the ad-hoc tribunals established that an aider or abettor does not need to share the principal perpetrator’s intent. It is sufficient that they knew their conduct would assist the commission of the crime. By contrast, the Rome Statute of the International Criminal Court appears, at least on the surface, to adopt a more demanding standard, requiring that assistance be provided “for the purpose of facilitating” the crime.

⁴⁰ [Blind Spot in the Boardroom – Why businesses ignore international criminal law, and why they shouldn’t, Gerald Pachoud, 2026.](#)

⁴¹ ICTY, Prosecutor v Furundžija (Trial Judgment) IT-95-17/1-T (10 December 1998) [234–235]; SCSL, Prosecutor v Charles Taylor (Appeals Judgment) SCSL-03-01-A (26 September 2013) [368–371], available at: <https://www.rscsl.org/Documents/Decisions/Taylor/Appeal/1389/SCSL-03-01-A-1389.pdf>.

⁴² See for e.g.: Kai Ambos, Treatise on international criminal law, vol I: Foundations and General Part (Oxford University Press 2013) 214–220; Elies van Sliedregt (2025); Nikola R Hajdin (2024). Sabine Michalowski, ‘The “Mens Rea” Standard for Corporate Aiding and Abetting Liability – Conclusions from international criminal law’ (2014) 18(2) UCLA Journal of International Law and Foreign Affairs 237, 237–74, available at: <https://www.jstor.org/stable/45302382>.

This difference in formulation has fuelled debate over whether the ICC requires proof of intent rather than mere knowledge. In practice, however, this distinction is less decisive than it might seem, particularly in cases involving corporate actors. Although important doctrinal differences remain across jurisdictions and tribunals, prosecutors and courts rarely look for explicit expressions of criminal purpose. Instead, they assess whether the company or its executives knew, or should reasonably have known, that their activities would contribute to international crimes, taking into account the surrounding context, including the nature of the conflict, the conduct of counterparties, and the abundance of publicly available warnings.

International jurisprudence has also made clear that deliberate ignorance does not shield an actor from liability. Where a business consciously avoids confirming facts that point to criminal conduct, or fails to investigate obvious red flags, such behaviour may be treated as wilful blindness and regarded as functionally equivalent to knowledge⁴³.

Substantial effect - This is the link between the assistance and the crime. Courts assess:

- *Nature of the support: Was it critical (e.g., weapons) or peripheral (e.g., general goods)?*
- *Proximity to the crime: How closely was the assistance tied to the criminal act?*
- *Duration and scale: Was it a one-off transaction or a sustained relationship?*
- *Context: Did the assistance occur in a setting where crimes were widely documented and foreseeable? For example, a company supplying cement to build a school in a war zone may not cross the threshold. Supplying the same cement for the construction of illegal settlements or military installations (knowing their purpose) likely does.”*

To consider adding:

- Section on domestic civil and criminal liabilities
- Section on legal risk relating to (commissioning or encouraging the commission of) bribery and corruption

⁴³ ICTY, Prosecutor v Furundžija establishing that aiding and abetting requires knowledge that one's conduct assists the commission of the crime; ICTY, Prosecutor v Tadić confirming that shared intent with the principal perpetrator is not required; Rome Statute of the International Criminal Court; ICC, Prosecutor v Bemba et al (Judgment pursuant to Article 74) ICC-01/05-01/13 (19 October 2016) [97–99], discussing the interpretation of Article 25(3)(c), available at: https://www.icc.cpi.int/sites/default/files/CourtRecords/CR2016_02238.PDF; ICTY, Prosecutor v Blaškić (Appeals Judgment) IT-95-14-A (29 July 2004) [41–42], recognising that deliberate ignorance or wilful blindness may satisfy the knowledge requirement, available at: <https://www.icty.org/x/cases/blaskic/acjug/en/bla-aj040729e.pdf>.