Principles for Responsible Defence Investment

Concept Note

November 2025

Contents

Introduction

This Concept Note identifies the urgent need for a set of global principles ('**Principles for Responsible Defence Investment**' or 'Principles') to help investors navigate the challenges of investing in defence-related companies. The Concept Note also proposes a process and structure for the development and implementation of these Principles.

This initiative will not try to reconcile the irreconcilable given the diversity of investor perspectives. It recognises the legitimacy of choosing not to invest in defence-related companies, and at the same time supports the potential for investors to **invest responsibly in defence-related companies within an appropriate framework**.

The development of these Principles has become necessary for several reasons: a growing push by states to increase investment in the defence sector in response to increased geopolitical tension; the evolving and increasingly fluid definition of what constitutes a defence investment, with major technology firms and startups increasingly engaging in defence-related activities; and the challenge of demonstrating responsible business conduct in a sector whose products and services are often used in armed conflict, whose clients are frequently domestic or foreign governments and where the system itself shields the sector from rigorous investor scrutiny.

Acknowledging the ongoing efforts to enhance responsible business conduct across the defence value chain and in relation to investments in conflict-affected and high-risk areas (highlighted in Annex 1), the Principles will have a strong **focus on the sector's downstream risks associated with product use and potential misuse**. This reflects the growing materiality of these risks for investors, and the notable absence of guidance in this area.

For the purposes of this paper, 'defence-related' includes companies in the broader ecosystem of commercial activities that are linked to the defence sector, e.g. communications systems, Artificial Intelligence (AI) and cyber security, alongside traditional defence companies. In terms of weapons, this paper envisages conventional, nuclear, controversial and emergent weapons, systems and platforms falling into the scope of the Principles, as well as dual use and defence-tech equipment.

The Concept Note is divided into four sections. The first and largest section outlines the geopolitical, definitional, normative and fiduciary **context** for defence-related investments, demonstrating the need for the Principles. The second section describes the **use cases** for the Principles, such as ensuring defence-related investments are aligned with international laws and norms and account for their operational context. The third section sets out the **development** of the Principles, including the proposed scope and consultation process. The fourth and final section focuses on the **implementation** of the Principles, including their promotion, the development of subsequent tools and resources to aid their implementation and the **opportunities for stakeholders to be involved**.

This Concept Note has been co-created by a group of investors and subject matter experts who agree that wherever investors are making investment and stewardship decisions on defence-related companies, whether asset allocation and due diligence, direct investment, exclusionary screening or voting, engagement or fund development, they should be doing so responsibly. To enable this, **we call on investors and wider stakeholders to support us in the development and implementation of robust and credible Principles and tools.**

Context

The Context section takes up a significant portion of the Concept Note. This reflects the complexity of the issues, while seeking to raise awareness of certain topics which investors may be less familiar with, such as International Humanitarian Law (IHL). This section covers the trends in defence spending, the changing nature of 'defence companies', the legal, regulatory and norms-based environment, the risks and implications of connections to conflict, and the status of responsible investment and defence.

Changing geopolitics as catalyst for investment in defence-related companies

Intensifying geopolitical tensions have forced states to reflect on existing security arrangements, with many now seeking to bolster their defence spending. In 2024, according to the Stockholm International Peace Research Institute (SIPRI), world military expenditure hit USD $2.7tn – an increase of 37% since 2015 – following ten years of consecutive growth. Some estimates forecast global military spending rising to between USD $4.7 and $6.6tn in

2035. Already, the European Union (EU) has announced its ReArm Europe Plan/Readiness 2030 to leverage €800bn in defence investment through increased national funding, new and existing financial instruments and the mobilisation of private capital. Similarly, the United Kingdom (UK) has said it will bring forward the defence spending target of 2.5% of GDP by 2027, with a pledge to increase this to 5% by 2035.

This 'unprecedented' rise in military expenditure has been reflected in the valuations of arms companies, even prior to the spending announcements by the EU and UK. In 2023, the world's 100 largest arms companies generated $632 billion in revenue, a 4.2% increase from the year before, according to SIPRI. Growth of the Aerospace and Defence sector is expected to continue, with innovations including AI-powered platforms, autonomous weapons systems and cybersecurity fundamentally changing what constitutes both a weapon and a defence company. A significant, albeit symbolic, display of how enmeshed technology and defence has become was the swearing in of four tech executives to the U.S. Army Reserves in June 2025 as part of 'Detachment 201', a unit which will advise the Army on technologies for potential use in combat.

It is not only governments investing in this space; private capital is also coalescing around the defence industry and especially defence technology. A report by McKinsey & Co. notes global venture capital investments in defence-related companies jumped by 33 percent year-over-year to USD $31bn in 2024. S&P analysis also showed there was USD $4.27bn of private equity and venture capital investment in aerospace and defence in the first quarter of 2025, compared to USD $4.31bn invested in all of 2024.

The sector is also drawing the attention of publicly backed finance vehicles. In June 2024 the North Atlantic Treaty Alliance (NATO) Innovation Fund, a multinational venture capital initiative, revealed its first investments focused on novel materials and manufacturing, AI, space and robotics – all fields relevant to defence innovation. Additionally, the Defence, Security and Resilience Bank (DSR Bank) was launched in March 2025 with a mandate to provide lower cost finance for NATO members and allies for investment in defence and related technologies. This multilateral lending institution – the first of its kind – also plans to mobilise private finance by underwriting investment in those areas for commercial banks. Several European pension funds have also announced they are reviewing their policies on weapons manufacturers, with pressure building on others to align with their own government's spending programs (e.g. Norway) and lift investment restrictions on companies involved in the manufacturing of certain weapons and components.

While certain recent conflicts and political developments have prompted significant rethinks in security and defence spending, particularly in Europe, this should be framed within a broader trend of conflict and violence. Since 2020, the level of conflict globally has doubled according to the Armed Conflict Location Event Dataset Project (ACLED), while the number of political violence incidents has increased by 25% from December 2023 to 2024. This changing security paradigm has been denoted a 'megatrend' by the European Commission, with methods of confrontation evolving in response to novel and emergent threats, changing the way that warfare is conducted (for example in the domains of space, cyber and information warfare).

In summary, there is **rising geopolitical uncertainty, substantial increases in defence-related spending, a trend of increased conflict and expanded domains where conflict happens**. These factors will undoubtedly affect the wider investment landscape**, demanding a reassessment of what it means to invest responsibly in the defence sector**. Given the increased financial flows and the sector's relatively attractive investment fundamentals, a set of Principles is needed to support investment decision-making and ensure that any revised approach remains consistent with broader responsible investment values.

Understanding what constitutes a defence-related investment

To appreciate how fluid the defence ecosystem has become, it's worth recalling the traditional structure and funding of defence companies. Historically these were often state-owned entities serving only government clients, with procurement driven by national security needs and contracts being long-term and highly regulated. In the post-Cold War era the sector underwent a period of significant consolidation, with a handful of large companies emerging as dominant players in the related fields of aerospace, maritime systems, electronic warfare etc.

Where previously defence companies focused on manufacturing military hardware (i.e. vehicles, weapons systems and communications equipment), which had high entry costs and took significant time to develop, recent attention and funding have shifted towards software-based platforms and low-cost platforms such as Unmanned Aerial Vehicles (UAVs or drones). This has significantly expanded what can be considered a defence-related company, further complicated by expanding 'dual use' technologies with both civilian and military applications.

Examples of this include speech-to-text translation and recommendation algorithms, originally developed for consumers, but now increasingly being used in autonomous weapons and intelligence analysis. More recently, concerns have been raised about cloud-based storage platforms and whether they constitute a 'dual-use' technology by enabling mass surveillance and targeting by military actors.

On the battlefield, UAVs have been reported to be central to both surveillance, targeting and strikes, with programs used for tracking and targeting enemy combatants becoming increasingly sophisticated and capable of operating with greater independence. Artificial Intelligence (AI) also plays a growing role, powering target recognition, predictive analytics, and decision-making processes, supported by companies traditionally not classed as 'defence companies'. Similarly, electronic warfare and deepfake propaganda are increasingly popular methods of offense, with cyberattacks targeting critical civilian infrastructure and military networks, and electronic systems being used to jam communications or disable drones, raising issues of responsible state cyberspace behaviour. The militarisation of space adds another layer of complexity, with both state and private actors deploying satellite systems which have become essential to national security infrastructure, as well as developing hypersonic missiles – which fly through near-space – and anti-satellite weapons.

For the Concept Note '**defence-related' includes companies in the broader ecosystem of commercial activities that are linked to the defence sector, e.g. communications systems, Artificial Intelligence (AI) and cyber security, alongside traditional defence companies.** This approach is aligned with the definition from the UN Working Group on Business and Human Rights ('Working Group' or 'UNWG'), which goes beyond a traditional framing of companies involved in weapons, related parts and services or military contracting.

As with previous military innovations, 21st century technology is fundamentally reshaping conflict dynamics in terms of how and where operations are conducted. The deepening integration of traditional defence and technology companies presents a spectrum of analytical and ethical challenges for investors, with attempts to distinguish between them through definitions and taxonomies becoming increasingly challenging. A set of responsible investment Principles focused on the specific merits and risks of a defence-related opportunity, in terms of product and conduct based analysis, will help investors address these definitional challenges.

Legal, regulatory and norms-based considerations for defence-related investments

The defence sector is governed by a patchwork of legal, regulatory and normative frameworks, including International Humanitarian Law (IHL), International Criminal Law (ICL), International Human Rights Law (IHRL), national / supranational legislation, treaties, licensing regimes and international business and human rights norms, with significant implications for both defence-related companies and their investors. The implementation of these instruments is inherently complex and highly context specific. Accordingly, this Note provides a high-level overview of their relevance to private enterprises engaging in defence-related activities.

IHL regulates conduct in armed conflict. **It is binding on States, as well as any business or individual conducting activities closely linked to armed conflict**. Companies face legal risk – including criminal or civil liability – if they fail to effectively comply with their IHL obligations. Examples of failings include pillaging resources, employing security forces that commit IHL violations, or supporting armed groups involved in war crimes. War crimes are serious breaches of IHL, whereby individuals may be held directly accountable for their actions. In these circumstances, the obligation to prosecute offenders primarily rests with the states that have jurisdiction. The International Criminal Court (ICC) may exercise jurisdiction under specific circumstance outlined within the Rome Statute. Under IHL and ICL, liability can also extend beyond direct perpetrators, to those who assist, plan, or instigate war crimes. Depending on the circumstance and jurisdiction businesses and business leaders may face legal risk if there is alleged 'complicity' in criminal activity (for example the recent Lafarge and Lundin cases).

Furthermore, any business found to be involved in the development, production or transfer of weapons that are prohibited by IHL may also risk legal sanction. While not universally defined, 'controversial weapons' is a term used in the investment industry for weapons which are widely prohibited under international treaties because they cause indiscriminate harm or violate core principles of IHL – such as distinction, proportionality and necessity. This term generally covers chemical and biological weapons, anti-personnel landmines, cluster munitions, blinding lasers, non-detectable fragments and incendiary weapons (e.g., white phosphorous), which are considered under various treaties, protocols and conventions. The production and transfer of nuclear weapons, systems, parts and technology are heavily restricted by agreements including the Treaty on the Prohibition of Nuclear Weapons (TPNW) and the Non-Proliferation Treaty (NPT), but they are not 'banned' in the same way as

chemical weapons or anti-personnel mines. The inclusion of nuclear weapons in 'controversial weapons' lists is not a given; investors and data providers take different approaches[1]. Controversial weapons are a complex topic which is further complicated by differentiations between the legality of **production**, **stockpiling** and **use** of weapons under IHL.

A complementary but distinct body of law to IHL is International Human Rights Law (IHRL). IHRL confirms the human rights of individuals and groups as codified in many major global treaties[2]. Companies should comply with IHRL independently from states' ability or willingness to do so. While IHL is applicable to both state and certain non-state actors during armed conflict**, IHRL applies in peace *and* conflict**, though certain provisions of IHRL can be derogated in times of public emergency. The UN Guiding Principles on Business and Human Rights (UNGPs) – a normative international framework – clarify the human rights responsibilities of states and business enterprises. The UNGPs stipulate that **all companies have a responsibility to respect internationally recognised human rights**. This responsibility comprises three key elements: adopting a human rights policy commitment; conducting human rights due diligence to identify, prevent, mitigate, and account for potential and actual adverse impacts throughout their value chains; and enabling the remediation of any business-related human rights harms.

The UNGPs have been legislated – in part – across several jurisdictions; mandating companies to conduct human rights due diligence and report on their related human rights risks and impacts. The UNGPs are complemented by the OECD Guidelines for Multinational Enterprises on Responsible Business Conduct (OECD Guidelines) and the ILO Tripartite Declaration of Principles concerning Multinational Enterprises and Social Policy (MNE Declaration), all three of which are the core reference points for responsible business conduct (RBC).

Supranationally, there has been a push to incorporate standards of responsible business conduct into the legislative environment of the European Union (EU). An example of this is the EU sustainable finance framework (EUSFF), a package of measures which includes the Corporate Sustainability Due Diligence Directive (CSDDD), the Corporate Sustainability Reporting Directive (CSRD), the EU Taxonomy Regulation (EU Taxonomy) and the Sustainable Finance Reporting Directive (SFDR). These measures seek to promote transparency and investment in economic activities considered to be sustainable in environmental and human terms, emphasising the need for operators and financial market participants to undertake human rights due diligence to assess Principle Adverse Impacts (PAIs) – including human rights violations (PAI 10) and exposure to controversial weapons (PAI 14) – and to ensure activities comply with Minimum Safeguards in relation to human rights. Initially it was unclear if investing in the defence sector was compatible with the requirements of the SFF, resulting in hesitancy by many financial firms to include the sector in their sustainability focused products, such as Article 8 and Article 9 funds. To address these concerns, the European Commission issued a notice which explicitly outlined how investment in the defence sector is compatible with the various aspects of the SFF.

At the national level, when it comes to the transfer of armaments, export licensing regimes – informed by agreements such as the Wassenaar Arrangement, EU Common Position on Arms Exports and UN Arms Trade Treaty (ATT) – are the primary instruments used by governments to ensure commercial activities are aligned with national interests and in compliance with applicable laws. Transfers in violation of these controls risk incurring civil or criminal penalties for the individuals and companies involved. This includes potential complicity in war crimes under national or international criminal laws when transferring weapons with knowledge, or the likelihood of which, they will be used to perpetrate specific violations of IHL. The International Committee of the Red Cross (ICRC) notes that similar considerations of mis-use should be applied to the sale of dual use products and services which may violate IHL, such as surveillance equipment and cyber-security software and the ICC has been developing its approach to 'cyber-enabled international crimes'.

---

[1] Note - some investors exclude companies involved in 'controversial weapons' through product-based screening, but the scope of exclusions will ultimately depend on what they choose to classify as 'controversial'. Recognising the wide variety of approaches by investors, nuclear weapons will be treated as a separate category to controversial weapons in the Principles, in line with the approach taken by the EU's Sustainable Finance Disclosure Regulation (SFDR).

[2] Including but not limited to the International Bill of Rights (which encompasses the Universal Declaration of Human Rights (UDHR), International Covenant on Civil and Political Rights (ICCPR), International Covenant on Economic, Social and Cultural Rights (ICESCR)), the Convention on the Rights of the Child, the Convention Against Torture and others.

Despite the potential for criminal sanctions, there have been several controversies relating to the transfer or sale of weapons to countries with poor human rights records[3]. This has led to criticism of export licensing regimes in relation to poor quality risk assessments, fragmented and inefficient governance and inadequate end-use monitoring, for example World Peace Foundation's critique of UK arms export controls. **Allocating capital to defence-related companies without addressing governance and human rights deficiencies risks undermining investors' own normative obligations and commitments**. This point was underscored by a group of UN experts in June 2024, who stated that failure by financial institutions to prevent or mitigate their business relationships with certain arms manufacturers "could move from being directly linked to human rights abuses to contributing to them, with repercussions for complicity in potential atrocity crimes".

A critical challenge posed by defence-related technologies is that they are evolving faster than the legal and regulatory frameworks designed to govern weapons and conflict, blurring the lines of accountability for harms incurred. This presents a real concern for investors, who may have relied on export licensing agreements – despite their well-documented deficiencies – as a proxy for understanding whether company actions are legally compliant and whether they are aligned with international human rights standards.

The legal, regulatory and norms-based context is complex and reflects multiple risks to investors, for whom a blanket reliance on existing laws or systems, such as export controls, will not sufficiently address those risks. The Principles may help navigate the complexity and support risk mitigation.

Business risks connected to armed conflict and implications for investors

As noted earlier, situations of armed conflict present unique challenges for companies exposed through their direct operations or value chain. Often, Conflict Affected and High-Risk Areas (CAHRAs) have already been impacted by unstable governance, clashes over control of territory and resources, or a heightened presence of private security actors or other non-state armed groups. The nature of defence-related businesses means that although they might not be directly involved in hostilities, they are frequently linked to CAHRA environments. This nexus presents an increased risk of being connected to human rights abuses [in peace times and contexts affected by violence but not classified as conflict], *as well as* violations of IHL [in classified armed conflicts, including situations of occupation], if not managed appropriately.

Under the UNGPs all business enterprises – including defence-related entities and their investors – have a responsibility to respect human rights. To meet these obligations, businesses should conduct human rights due diligence to identify, prevent, mitigate and account for how they address impacts on human rights. Guiding Principle 12 notes that during armed conflict, enterprises should respect the standards of international humanitarian law and Guiding Principle 23 notes that businesses should comply with IHRL even when the state does not. This can mean that compliance with state law is not sufficient for a business to discharge its responsibility to respect human rights.

As explained in the guide produced by the UN Development Programme and the UN Working Group on Business and Human Rights, 'Heightened Human Rights Due Diligence for Business in Conflict-Affected Contexts', the complexity of this process is built around the concept of proportionality, i.e. the higher the risk, the more complex the process needed. In conflict-affected areas, human rights due diligence should be 'heightened' to account for the increased risk of being involved in serious human rights abuses. This demands identification not only of the potential and actual impacts on people, but also how business activities might be affecting the conflict or exacerbating hostilities. By taking these actions, businesses can avoid causing, contributing or being linked to an adverse human rights impact. Failure to do so potentially incurs a variety of risks for both companies and investors:

- **Investment/Financial risks** – These legal and reputational risks can impact a business's commercial success and value if they are not appropriately managed. Firms who are seen as behaving unethically, especially in the context of armed conflicts or civil unrest could face backlash from clients, consumers, civil society, or other governments, negatively affecting financial performance. Additionally, where such behaviour is unlawful firms face financial penalties or even criminal

[3] For examples see The Weapons Industry Kills: How U.S. Corporations Export Death Around the World - Harvard Law School | Systemic Justice Project, Out of Control: Irresponsible weapons transfers and future weapons systems, Exporting risk: how UK arms sales overlap with countries using explosive weapons in populated areas

prosecution which can impact organisational stability and profitability, thereby affecting the investment value.

- **Reputational risks** – The credibility of businesses and investors can be affected where they are perceived to mishandle human rights issues, particularly in contexts involving armed conflict and potential links to international crimes. These situations – intensified by public and media scrutiny – signal poor risk management, can damage relationships with clients, fund members, and regulators, and can be a distraction to management and impact staff engagement, potentially leading to financial loss and undermining their social licence to operate.
- **Legal risks** – Businesses in certain jurisdictions risk financial penalties for failing to undertake human rights due diligence and report on their risks and impacts. The same is true for investors whose activities fall under sustainable finance regulations. Additionally, breaches of IHL obligations potentially expose a company – and its individual officers – to civil or criminal liability. Targeted sanctions have also been used by governments against individuals and businesses engaging in 'egregious conduct' often in areas affected by conflict.
- **Systemic risks** – Businesses and investors depend on well-functioning financial markets to allocate capital efficiently, manage risk, and drive economic growth. These markets, in turn, rely on stable economies and cohesive societies to function effectively. However, widespread human rights violations – particularly those associated with armed conflict – can undermine macroeconomic stability and ultimately threaten the integrity and resilience of financial systems, presenting significant risk to business and investors alike.

In spite of these risks, the UNWG observes that the majority of defence-related businesses are still failing to conduct basic – let alone 'heightened' – human rights due diligence, with respect to arms production and transfers, and that "identification of risks of negative impacts by virtue of the use of their products or services in different places and conflicts is still largely absent". This should greatly concern investors looking to deploy capital into the space, considering their own responsibilities to avoid causing or contributing to human rights harms as well as the potential negative impacts on returns and consequences for breaching fiduciary duties.

To mitigate these risks, a set of Principles could provide a framework for making defence-related investment decisions - particularly in relation to down-stream due diligence and potential end use risks.

The status of responsible defence investing defence

The concept of Responsible Investment (RI) has different meanings for different people. In broad terms, RI requires investors to incorporate environmental, social and governance (ESG) factors into their investment decisions and stewardship activities. Objectives for those looking to invest responsibly can include managing risk to their portfolios, aligning with ethical values, and delivering measurable social or environmental outcomes. The approaches taken to achieving these objectives will vary depending on the investment thesis and asset class. The approaches can cover, for example, excluding certain sectors or companies, integrating sustainability factors into financial analysis, and engaging with investee companies to improve their practices over time.

Investors have had multiple reasons **for not allocating** capital to the defence sector as set out below[4]:

- **Ethical exclusions** – Investors, for example faith-based asset owners, can have policies excluding certain defence investments which are typically underpinned by ethical or theological reasonings.
- **Norms-based exclusions** – Investors can have norms-based exclusions policies, which exclude companies seen to be in violation of international norms (such as the UN Global Compact and the OECD Guidelines), which may capture certain defence-related companies, particularly those involved in controversial weapons. Certain sustainability focused funds may have similar exclusions.
- **Client mandates** – Investors may have a personal preference to not have their assets allocated to certain types of companies, including defence companies, and asset managers provide investment vehicles which meet their clients' requirements.
- **Reputational risk management** – Investors have come under scrutiny from media and civil society organisations for holding stock in defence-related companies involved in the development of

[4] Note that these approaches are not thought to have hindered investment in the defence industry, as explained in the recent Royal United Services Institute report 'Are ESG Standards the Scapegoat for Stalling Defence Growth?'

controversial weapons or the supply of arms and equipment to states involved in ongoing conflicts, which may lead to exclusions.

- **Legal risk management** – The legal and regulatory context may lead investors to exclude companies as both a compliance and legal-risk management response.

Since the full-scale invasion of Ukraine in 2022, several investors have relaxed or removed historic restrictions on conventional defence companies. Those investors are largely also part of initiatives, such as the Principles for Responsible Investment (PRI) and therefore committed to 'RI', while also choosing to allocate capital to defence-related companies. Whatever the reasons for investing in defence (e.g., benefiting from growth in the industry, following government direction, responding to client demand or wishing to support domestic security), investors need to implement approaches that are appropriate for defence-related companies, and which address the specific risks and dilemmas related to the sector.

To date, the RI community has given limited attention to defence companies, particularly regarding the downstream sale and use of their products and services. This is partly due to the sector's elevated risks – such as human rights violations, corruption and environmental harm – which investors have often avoided through exclusions and the reliance on export controls, and partly due to the nature of the industry in terms of its unique relationship with government. Recent initiatives, such as the UK Defence ESG Charter, focus primarily on operations and supply chain ESG/Sustainability issues and while it touches on the risks of end-users, human rights due diligence or connections to breaches of IHL are not discussed. The US Defence Industry Initiative on Business Ethics and Conduct (DII Principles), last updated in 2010, focuses heavily on things like supplier codes of conduct, anti-bribery and corruption, and rules for selling to government, but the end-use of products and services do not appear to feature. It can be argued that the industry, due to its relationship with government and export controls, has a shortened view of its own responsibilities, but **investors need to look deeper into the downstream value chain to manage their own financial, human rights, reputational and legal risks**.

Despite the inherently high human rights risks for defence companies, initiatives such as the Corporate Human Rights Benchmark, used by investors to assess, rank and engage with high-risk companies, have avoided the sector due to the down-stream nature of the risks. While there are a wide range of tools to support investors considering risks related to conflict e.g., the Investor Toolkit on Human Rights and Armed Conflict, and the Saliency Materiality Nexus, these were designed to deal with companies exposed to CAHRAs, as opposed to companies who, for example, manufacture and supply weapons or are part of the military 'kill-chain'. Collaborative engagements have also taken leading approaches to investor engagement on the topic of CAHRA, but as yet there is no sector / risk specific central framework for investors to convene around that would enable an informed and coherent approach to help integrate responsible investment for defence-related companies and guide stewardship or engagement.

A further challenge is the lack of reliable data to support decision making on defence-related investments. As explained to the UN Human Rights Council, the unique business models of defence companies – marked by their close interrelation with national security and inherent confidentiality obligations – make them notoriously opaque, particularly in disclosing information on risk management and human rights due diligence. This opacity is driven by several factors: limited accountability for States in upholding human rights provisions within arms control laws; poor transparency in relation to arms exports globally; corruption risks within the sector; insufficient human rights due diligence by arms companies; and the failure by States to mandate such practices. As a result, investors often rely on research produced by ESG data providers (Providers), which introduces a new set of issues.

Despite current efforts to rationalise, a lack of consistency and corporate transparency remains a problem across the ESG data landscape. Without a universally accepted standard across ratings agencies and indices, ESG metrics are often applied inconsistently. This problem is further complicated by business involvement in dual-use technologies, as it becomes difficult to distinguish clear lines between responsible business practices, such as selling commercial drones to the civilian market, and practices that could contribute to human rights harms and abuses during conflicts, such as selling drones that can be customised and militarised for use on the battlefield. These providers are also not immune from the political pressures faced by companies and investors, with several rolling back data offerings relating to conflict-affected areas, for example Sustainalytics.

Investors seeking to responsibly allocate capital to defence-related companies face a litany of challenges when it comes to decision useful data. The increased complexity of defence-related companies – particularly those involved in dual-use technology – has made analysis of these companies more resource intensive. This challenge

has been compounded by the rollback of ESG data provision on topics highly material to defence-related companies, which already suffered from a lack of transparency and inconsistencies in interpretation. As such, there are gaps in terms of data, tools, collaborations and convening principles, which need to be addressed if responsible investment approaches are to be applied to defence-related companies. The Principles may help create the momentum to address these gaps, if enough investors are asking for the same thing.

The context is complex and dynamic. Investors face significant risks connected to defence-related investments and there are significant challenges in addressing those risks. A set of robust Principles, implemented by a critical mass of investors, can help navigate the complexity and mitigate the financial, reputational, legal and human rights risks. The next section explores what the use cases for the Principles could be.

Use cases for the Principles

As explained above, there are distinct risks and challenges connected with defence-related investments and there are clear gaps in terms of responsible investment practices to address them. A set of global, credible, investor-led Principles can provide the starting point to meet this challenge, enabling investors to cohere around a common framework. At a broad level, the Principles should support the respect for global norms, which aligns with both government duties, company and investor responsibilities and societal expectations. Providing much-needed guidance and coherence, the Principles should help investors navigate the complex intersection of national security, human rights, and responsible business conduct and help ensure that capital flows to defence-related businesses are done in a way that aligns with expectations on responsible business conduct. Additionally, the Principles should help investors manage the risks and implications of investing in defence-related companies (financial, legal, reputational and social), especially where investee companies are connected to armed conflicts.

The table below summarises various use cases for the Principles, although the relevance of the activities will be dependent on the specific investor, their mandate, investment style, portfolio and resources:

Area	Use case
Policy	To inform the development, or update, of relevant internal policies, making commitments explicit to internal and relevant external stakeholders, helping to meet relevant legal obligations and ensuring a systematic approach that is grounded in emerging good practice.
Risk assessment	To help identify and assess potential reputational, financial and legal risks associated with defence-related investment(s), for example the manufacture or supply of weapons used in contravention of IHL.
Investment Due Diligence	To enhance pre-investment due diligence of defence-related investment(s), or of managers and funds with a defence focus, augmenting compliance with sanction regimes, export controls and related financial regulations.
Human Rights Due Diligence	To inform human rights due diligence approaches to identify where investors are connected to companies causing, contributing to or directly linked to adverse human rights impacts, and take appropriate action. In situations of conflict, they could be used to support heightened human rights due diligence.
Product Development	To inform the development of funds or investment products, and to ensure alignment with regulated funds and disclosure standards.
Screening	To enhance screening processes, providing more nuanced criteria (e.g. for clients) and moving beyond a blunt product and revenue-based exclusion process.
Company Engagement and Stewardship	To support the creation of coherent frameworks that can be used to assess and engage (bilaterally and collaboratively) with defence-related companies on their policies, processes and actions, in ways that are appropriate to owners and managers across public and private investments.
Divestment	To support divestment decision making for investee companies where, for example, company conduct is not in line with global norms and where engagement has failed.
Remedy	To support investors to meet their responsibilities under the 'access to remedy' pillar of the UNGPs, e.g. engaging where remedies to rightsholders are not available from the invested business.

Area	Use case
Reporting and Client Engagement	To inform clients and the broader market about how the investor has fulfilled their responsible investment responsibilities and commitments when allocating capital to defence-related investments.
Multi Stakeholder Collaboration	To support the convening of investor, government, industry and civil society stakeholders to advance responsible business conduct in the sector. The Principles could provide a simple reference point for stakeholders to understand investor perspectives.
Data Landscape	To guide coherent requests of ESG Data Providers in terms of defence-related company data and internal methodologies and approaches.

Development of the Principles

Proposals and assumptions

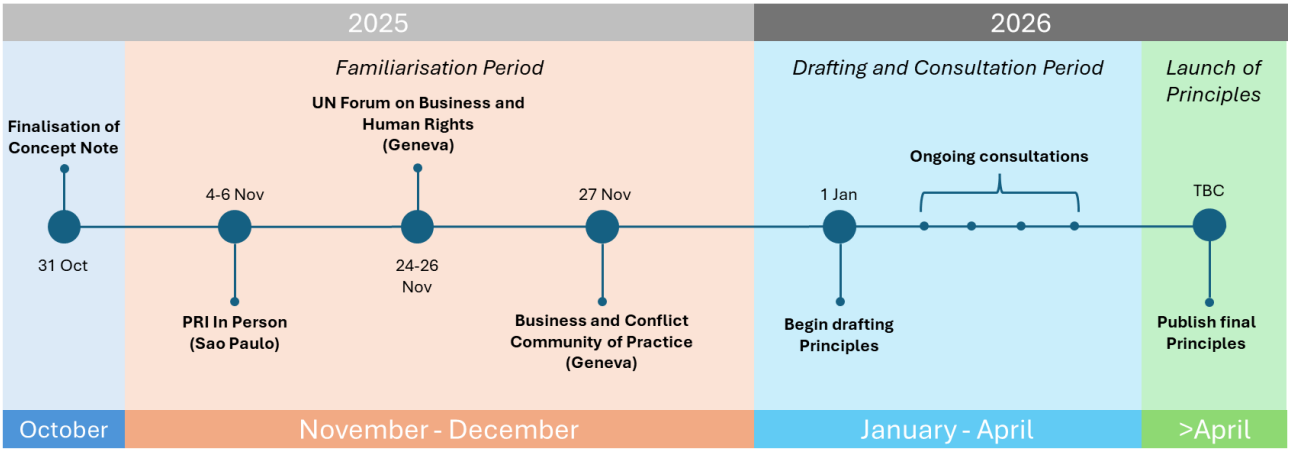
It is necessary to confirm the required scope of the Principles and in what way they can be best implemented before creating a detailed first draft. As such, this section sets out some high-level proposals, designed to guide their development, set their scope and shape their success:

- **Guiding star -** The Principles will be anchored in international humanitarian law (IHL) and the UN Guiding Principles on Business and Human Rights (UNGPs), and they will support the alignment of investor activity with international norms. Robust human rights due diligence will be a cornerstone of responsible defence investment activities.
- **Investor scope –** The Principles will support both asset owners and asset managers in integrating responsible investment for defence-related companies in both public and private markets. To meet this need they will have to be broadly applicable, but practically implementable.
- **Activity scope –** The Principles will apply to all contexts (i.e. not just in conflict) and will consider the full range of responsible-investment and stewardship decision making (including due diligence, screening, engagement, voting, fund development and reporting). While not encouraging or prohibiting specific courses of action, such as engagement or exclusion, the Principles should enable investors to take those actions in ways that align with international norms and good responsible-investment practices.
- **Company scope** – The Principles will support responsible investment for a wide range of companies that are connected to defence and conflict, including: companies that are involved in the manufacture, sale, distribution and support of conventional and controversial weapons and platforms, and their suppliers/supply chain; companies that provide or export 'non-weapons' services or goods to the military, such as dual-use equipment and defence-tech.
- **Issue scope** – The Principles will consider a broad range of issues including:
  - Violations of international law, including the production of weapons banned by treaty, the use of indiscriminate weapons or unlawful use of force.
  - The evaluation and integration of environmental, social and governance risks across company value chains, including: the environmental impact of production and operations; the social risks such as misuse of products and workforce practices; and the governance issues such as anti-corruption, lobbying and the role of governments through licenses, export controls and contracts.
  - The intended and actual use of products and services and the extent to which defence-related companies are acting in accordance with international standards on business and human rights, such as the OECD Guidelines and the UN Guiding Principles on Business and Human Rights.
- **Building consensus –** The Principles will be voluntary but should create a broad consensus on what is expected across the various investment and stewardship activities for defence-related companies. The Principles should also set, or refer to, common expectations of defence-related companies. The Principles will be informed by stakeholder input and consultation.
- **Maximising success –** Noting the complexity of the sector, success is more likely if there is significant uptake by investors and buy-in from stakeholders (including governments, industry, civil society and investor initiatives), which may be best achieved through the creation of stand-alone initiative or body to own the Principles and support their implementation.

Co-Development: Familiarisation and consultation periods

The Principles will need to work for a broad range of investors, while being credible to a wide range of stakeholders. Following the publication of this Concept Note, there will be a familiarisation period to gather input on the structure and scope of the Principles and the best approach to ensure successful implementation. A co-development timeline is set out in the image below.

During the Familiarisation period, the PRDI Initiating Group will seek feedback, primarily from the investor community, on the proposals in this Concept Note and appetite for future involvement. Annex 3 contains a list of indicative questions which will be raised at various events or in surveys. Drawing on inputs from the familiarisation period, a draft set of Principles will be published in 2026 and used, alongside this Concept Note, to drive consultations with investors and investor initiatives, industry associations and defence-related companies, governments and policy makers, civil society and relevant subject matter experts. If required, a more formalised structure will be created to oversee the development and finalisation of the Principles and any implementing initiative.



Implementation of the Principles

The implementation of the Principles will be determined by the final shape and content of the Principles, as well as the framework that they end up operating under. There are several potential pathways for the PRDI, each with their own benefits and limitations, which will be explored during the consultation process. To help frame the future discussions, several pathways are set out below, each using a current example to explain a potential approach.

Membership Body with Certification and Compliance Mechanisms – The first pathway could reflect the International Code of Conduct Association (ICoCA). The ICoCA was created to oversee and implement the International Code of Conduct for Private Security Service Providers. It monitors member companies (analogous to investors for PRDI) to ensure compliance with the Code and also provides an accountability mechanism. The Code would be analogous to the Principles, and the Association would be analogous to a formal body that would oversee implementation of the Principles. This approach has very high startup and maintenance costs, while its effectiveness would likely depend on third parties requiring investors to be certified to an independent standard, and investors volunteering to be bound by such a standard.

A Multi-Stakeholder Initiative with a Standard – The second pathway could reflect the Voluntary Principles on Security and Human Rights Initiative (Voluntary Principles Initiative). The Initiative developed Voluntary Principles which later became a globally recognised standard (analogous to 'our' Principles). Company participants (analogous to investors) in the Initiative are responsible for implementing the Voluntary Principles and there is a formal application process, a requirement to commit to implement the Voluntary Principles and a level of ongoing monitoring. A Secretariat is responsible for day-to-day administration. The Initiative convenes key stakeholders from industry, government and civil society to advance implementation of the Principles, but the Initiative is not responsible for certification/audit of member companies. Non-members can use the Voluntary Principles. This approach has high start-up and maintenance costs but provides lower barriers to participation for companies than ICoCA. It requires multi-stakeholder buy-in but also provides a multi-stakeholder forum for advancing outcomes.

Membership Initiative with Lower Oversight – The UN Global Compact is a multistakeholder sustainability initiative, with a focus on corporates who commit to implementing a voluntary framework (the Ten Principles of the Global Compact – analogous to the Principles). Companies (analogous to investors) must submit annual progress reports (or risk delisting), and the organisation may remove participants where there are serious concerns, but there is no formal oversight mechanism for the implementation of the Principles. The organisation helps advance implementation of the Principles by supporting peer learning, working groups, guidance etc. It has a lower bar to entry and forced exit compared to, for example, the Voluntary Principles, but it arguably has a lower level of accountability or confidence in the application of the Principles.

Hosted Guidance and Toolkits – The Investor Toolkit on Human Rights and Armed Conflict was produced by the Responsible Investment Association Australasia (RIAA). It is designed to help all interested investors to manage human rights impacts and IHL implications related to conflicts. Toolkits are useful resources, but to create significant change they require broad uptake by investors, which would require the active support of collaborative investor initiatives, such as PRI Advance or Nature Action 100. They can also be limited in terms of broader stakeholder engagement and penetration across different stakeholder groups. Toolkits are relatively low cost to develop and maintain and can be housed within pre-existing initiatives such as RIAA or the Investor Alliance for Human Rights.

Choosing the right pathway will maximise the likelihood that investors will be able to navigate the complex context and manage the legal, financial, reputational and human rights risks of defence-related investments.

Invitation to contribute

This concept note has been co-created by a small group of investors and subject matter experts (detailed at Annex A). The Principles for Responsible Defence Investment, as well as any supporting initiative, will remain a concept unless stakeholders – especially investors – support their development and implementation. As the pressure to invest in defence increases, so does the need to invest responsibly, and now is the time to ensure that happens. To be part of the conversation and stay up to date, please complete this **Form**. If your organisation could provide resources to support the development and implementation of the Principles, please contact prdi@eiriscrn.org.

----------END----------

Annexes

Annex 1 - Frameworks and guidance relevant to defence-related companies

Annex 2 - Initiating Group

Annex 3 - Familiarisation questions

Annex 1 - Frameworks and guidance relevant to defence-related companies

The table below provides a non-exhaustive list of frameworks and guidance which speak to pre-existing efforts to advance responsible business conduct across both defence-related companies and companies operating in conflict-affected and high-risk areas:

Resource	Organisation	Scope	Comment
Defense Industry Human Rights Due Diligence Guidance	American Bar Association Center for Human Rights	Downstream	Guidance to assist defence exporters in preventing the misuse of their products and services
UK Defence ESG Charter	ADS	Value Chain	Set of ESG related commitments for UK defence companies
Defence Companies Index	Transparency International	Value Chain	The DCI assesses commitment to anti-corruption and transparency by the world's largest defence companies.
Responsible business conduct in the arms sector: Ensuring business practice in line with the UN Guiding Principles on Business and Human Rights	UN Working Group on Business and Human Rights	Downstream	Information Note outlining the challenges of integrating respect for human rights into the arms sector, with recommendations for state and business.
Heightened Human Rights Due Diligence for Business in Conflict-Affected Contexts	UNDP	Value Chain	Guidance to businesses and other actors on how to meet their responsibilities to carry out a heightened version of human rights due diligence in conflict-affected areas.
Investor Toolkit on Human Rights and Armed Conflict	Responsible Investment Association Australasia	Value Chain	Toolkit offering frameworks and insights for companies and investors to support human rights in conflict-affected regions.
The Saliency Materiality Nexus	Heartland Initiative, Wespath Benefits and Investments, Schroders	Value Chain	White paper describing how salient human rights and material risks intersect in Conflict-Affected High-Risk Areas.
Navigating Portfolio Exposure to Conflict-Affected and High-Risk Areas: Practical Guidance for Investor Engagement with Companies	Investor Alliance for Human Rights, Heartland Initiative, PeaceNexus	Value Chain	Practical guidance and best practice examples for investors seeking to identify, assess, prioritise and engage on CAHRA risks across their portfolios

Annex 2 - Initiating Group

The individuals listed below are the Initiating Group for the PRDI and have supported the development of this Concept Note. Where an individual has been acting in a personal, rather than organisational capacity, they are labelled as 'independent'. The participating investors act independently but manage over USD $5tn of capital.

Name	Organisation / Independent	Position
Angus Sargent	Church Commissioners for England (UK)	Senior RI Analyst (*former*)
Bennett Freeman	Independent	Former Vice President, Calvert Investments
Camille Bisconte de St Julien	LBP Asset Management (France)	Human Rights and Social Lead
Chloe Maury	Personal capacity	ESG Analyst, Amundi Investment Solutions
Dan Neale	Church Commissioners for England (UK)	Social Lead
Florence Foster	Geneva Academy of International Humanitarian Law and Human Rights Law (*in her personal capacity*)	Senior Project Manager
Kate Turner	First Sentier Investors (Australia)	Global Head of Responsible Investment
Jonathan Kolieb	RMIT University, Business and Human Rights Centre	Director
Katie Frame	Schroders (UK)	Engagement Lead
Luda Svystunova	Personal capacity	Head of Social Research, Amundi Investment Solutions
Peter Webster	EIRIS Foundation / EIRIS Conflict Risk Network	Chief Executive Officer
Rebecca DeWinter Schmitt	Investor Alliance for Human Rights	Associate Director
Samantha Chua	EIRIS Conflict Risk Network	Project Manager
Samuel Jones	Heartland Initiative	President
Sinisa Milatovic	Personal capacity	Business and Human Rights Specialist
Therese Sandmark	Skandia	Senior ESG Analyst
Withheld	Institutional Investor (Nordic financial services group)	Withheld
Withheld	Institutional Investor (French asset manager)	Withheld
Withheld	Institutional Investor (Global asset manager)	Withheld

In the development process, the following expectations were agreed by participants:

- Participants are expected to act with high standards of integrity and professionalism.
- All participants shall disclose any potential conflicts of interest that could influence their contributions or decision-making within the group.
- Given the sensitive nature of this topic, confidentiality must be respected at all times; sensitive information shared during discussions is to remain within the group unless explicitly agreed otherwise. This does not prevent participants from discussing the project in general with third parties.
- Participation in this project is at the discretion of individuals acting in either their professional or personal capacity and participants will disclose which capacity they are acting in.
- This project does not require or seek collective decision-making in, or action with respect to, acquiring, holding, disposing and/or voting of securities. All relevant participants will ensure compliance with applicable competition and anti-trust laws.

This Concept Note is a collaborative effort, and it should not be read as representing the official position of any of the organisations or participants listed above.

Annex 3 - Familiarisation questions

The following questions will be used to guide discussions following the publication of the Concept Note:

- Can you support the development of Principles and Tools, through participation in or supporting consultations, promoting them to wider stakeholders, or financial support to ensure their viability?

- Which of the use cases, as described in ***Table 1***, are most important for investors considering defence-related investment opportunities? Are there additional use cases not mentioned in this Concept Note that should be considered when developing the Principles?

- Does this Concept Note accurately reflect the challenges investors face when it comes to defence-related companies? Are there challenges missing from the Concept Note?

- What level of detail in the Principles would be most useful for investors:
  - Should the Principles set expectations for investors when allocating capital to defence-related companies, or should they focus more on expectations for defence-related companies themselves?
  - How proscriptive should the Principles be in defining expectations?

- Is the proposed scope correct? What should be covered in terms of:
  - The range of investor activities (screening, engagement, due diligence etc.).
  - The range of issues e.g. the integration of environmental, social and governance issues across the full value chain of a company, vs the focus on downstream due diligence.

- Which of the pathways set out in the Implementation of the Principles section will be most feasible and useful?

- Is PRDI / Principles for Responsible Defence Investment the most appropriate name?