SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
VOL. 3, ISSUE 10, APRIL 2026
Available Online : https://shodhprakashan.in/

The Ethics of Geopolitical Neutrality: Corporate Responsibility vs. National Security in Modern Warfare

Parhlad Singh Ahluwalia, Academician, Dr. Bhimrao Ambedkar Law University, Jaipur, Rajasthan, India

Abstract

The accelerating entanglement of multinational corporations in the infrastructure of modern warfare has destabilised the long-held assumption that private enterprise can remain neutral in geopolitical conflict. Cloud computing platforms, satellite communication networks, semiconductor supply chains, and social media ecosystems are now load-bearing components of national defence, transforming corporations from passive bystanders into active — if reluctant — belligerent-adjacent actors. This paper examines the ethical tension between corporate claims to geopolitical neutrality and the practical demands of national security in the context of modern, technologically mediated warfare. Using a qualitative, document-based case-study methodology, the paper analyses the behaviour of major technology firms during the 2022 Russian invasion of Ukraine, the contested role of Starlink in battlefield communications, the evolving treatment of the defence sector within Environmental, Social and Governance (ESG) investment frameworks, and the historical precedent of corporate disengagement from apartheid-era South Africa. Drawing on stakeholder theory, shareholder-primacy theory, the United Nations Guiding Principles on Business and Human Rights, and Just War theory, the paper develops a four-quadrant analytical framework — the Corporate Neutrality Spectrum — that classifies firm behaviour according to the degree of voluntary alignment with state security objectives and the depth of human-rights due diligence performed. The analysis finds that genuine corporate neutrality is, in practice, unattainable once a firm's infrastructure becomes militarily consequential; the meaningful ethical question is not whether to take a side, but through what governance process, with what transparency, and with what accountability that side is chosen. The paper concludes with policy recommendations for firms, investors, and regulators, and identifies avenues for further empirical research, including firm-level surveys and comparative regulatory analysis across jurisdictions.

Keywords: *corporate social responsibility; geopolitical neutrality; national security; dual-use technology; business and human rights; stakeholder theory; export controls; ESG; Ukraine; Starlink, Business Ethics, International Security, and Corporate Governance*

1. Introduction

Corporations have never been perfectly neutral actors, but the twenty-first century has exposed the fiction of corporate neutrality with unusual clarity. When Russian forces crossed into Ukraine in February 2022, the decisive early battles were fought not only with artillery and armour but with satellite bandwidth, cloud servers, and payment rails controlled by private

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
Vol. 3, Issue 10, April 2026
Available Online : https://shodhprakashan.in/

firms headquartered thousands of kilometres from the front line [1]. Within a month, more than 400 companies — and within a year, over 1,000 — had announced some form of withdrawal from the Russian market, a corporate exodus without precedent in scale or speed [2,3]. Microsoft suspended new sales, restricted state media, and simultaneously handed Ukrainian officials real-time cyber-threat intelligence [4,5]. Apple disabled live traffic data in Ukraine to prevent its exploitation for targeting while halting all commercial activity in Russia [1]. SpaceX's Starlink constellation became, almost by accident, the nervous system of Ukrainian battlefield communications, placing a private citizen in the position of adjudicating which military operations a sovereign state could technically execute [6,7].

These episodes crystallise a deeper structural shift. For most of the industrial era, "national security" and "corporate strategy" occupied largely separate domains: governments built weapons and negotiated alliances, while firms sold goods and services across borders with comparatively little exposure to the machinery of war. Dual-use technology — items or software that carry both civilian and military applications — has closed that gap. Semiconductors, cloud infrastructure, satellite constellations, encryption software, and even consumer mapping applications now sit squarely within what the United States Department of State's Bureau of Arms Control and Nonproliferation defines as "dual-use" goods subject to export licensing and diversion controls [8]. The Stockholm International Peace Research Institute (SIPRI) notes that its dual-use and arms trade control research increasingly extends beyond weapons of mass destruction proliferation into cyber-surveillance systems and the broader architecture of digital infrastructure [9]. Consequently, a company that has no intention of participating in warfare may nonetheless discover that its ordinary commercial product has become militarily indispensable — as Starlink did in Ukraine — or that its supply chain decisions are now, by operation of law, foreign-policy decisions [10,11].

This paper interrogates the resulting ethical dilemma: can a corporation claim geopolitical neutrality once its products or services materially affect the outcome of an armed conflict, and if not, what obligations should guide the choices it is forced to make? The question sits at the intersection of three literatures that have historically developed in relative isolation from one another — corporate social responsibility (CSR) theory, international humanitarian and human rights law as applied to business, and strategic studies concerned with the privatisation of security functions. The paper's central argument is that geopolitical neutrality, understood as genuine non-alignment with any belligerent party, is largely illusory for firms whose products possess strategic utility; what remains meaningfully contestable — and therefore what deserves ethical and regulatory attention — is the *process* by which firms decide whose side their infrastructure will, in effect, serve, and the *accountability structures* that govern that decision.

The paper proceeds as follows. Section 2 reviews the relevant theoretical and empirical literature, spanning shareholder-primacy and stakeholder theory, the United Nations Guiding Principles on Business and Human Rights (UNGPs), and the historical precedent of corporate disengagement from apartheid South Africa. Section 3 develops a conceptual framework — the Corporate Neutrality Spectrum — for classifying corporate conduct in conflict settings. Section 4 outlines the paper's qualitative case-study methodology. Section 5 presents four case studies: the 2022 corporate exodus from Russia, the Starlink controversy, the treatment of the defence sector in ESG investment frameworks, and the export-control regime as an external constraint on corporate discretion. Section 6 analyses the resulting data, including original tabulation of the Yale Chief Executive Leadership Institute (CELI) dataset and SIPRI military expenditure figures. Section 7 discusses the findings from four competing ethical and theoretical perspectives. Section 8 draws out policy implications for firms, investors, and states. Section 9 acknowledges the study's limitations, and Section 10 concludes.

2. Literature Review

2.1 Theoretical Foundations: Shareholder Primacy versus Stakeholder Theory

The modern debate over corporate responsibility traces most directly to Milton Friedman's 1970 essay in *The New York Times Magazine*, in which he argued that the only social responsibility of business is to increase its profits within the rules of the game, understood as open and free competition without deception or fraud [12,13]. Friedman's position, often labelled the "shareholder primacy" or "Friedman doctrine," holds that corporate executives are agents of shareholders and lack the democratic mandate to impose their own conceptions of the social good — including foreign-policy judgments — on the enterprises they manage [14]. Contemporary scholarship, however, cautions against a crude reading of Friedman's argument. Hühn observes that Friedman explicitly conditioned profit-seeking on conformity with "the basic rules of society," both legal and ethical, a qualification frequently elided in popular invocations of the doctrine [13]. Ferrero similarly argues that later attempts to fold Friedman into stakeholder theory — as Freeman himself once proposed — misrepresent Friedman's actual commitments, which reserve instrumental concern for non-shareholder interests only insofar as they serve shareholder value [14].

R. Edward Freeman's stakeholder theory, first systematised in *Strategic Management: A Stakeholder Approach* (1984), redirects the locus of managerial obligation from shareholders alone to the full constellation of groups with a stake in the firm's conduct: employees, customers, suppliers, communities, and — by extension in the conflict context — the civilian populations affected by a firm's products [15,16]. Under stakeholder theory, a cloud-computing firm whose infrastructure hosts military command-and-control functions bears a moral relationship not only to its shareholders and paying customers but to the soldiers and civilians whose lives are affected by the reliability, availability, or withdrawal of that infrastructure. This paper treats the Friedman–Freeman axis not as a binary choice but as a continuum against which observed corporate conduct in wartime can be plotted, a point developed further in Section 3.

2.2 The Business and Human Rights Framework

A second and increasingly authoritative body of literature has emerged around the United Nations Guiding Principles on Business and Human Rights (UNGPs), endorsed by the UN Human Rights Council in 2011. The UNGPs rest on three pillars: the state duty to protect human rights, the corporate responsibility to respect human rights, and access to remedy for victims of business-related abuse [17]. Guiding Principle 12's commentary specifies that the scope of the corporate responsibility to respect expands in situations of armed conflict, where enterprises are expected to observe the standards of international humanitarian law even where the state itself may be failing to do so [18]. Davis's influential analysis of the UNGPs in conflict-affected areas emphasises that businesses "invariably impact the dynamics of a conflict," whether by supplying revenue to a combatant government, providing dual-use infrastructure, or withdrawing services in ways that have humanitarian consequences of their own [19].

Building on this foundation, the UN Working Group on Business and Human Rights, in partnership with the UN Development Programme, published a dedicated guide to "heightened human rights due diligence" (hHRDD) for enterprises operating in conflict-affected contexts [20,21]. The guide instructs firms to identify "warning signs and triggers" for escalated risk-assessment, to adopt conflict-sensitive practices, and to track the effectiveness of their mitigation measures on an ongoing basis rather than through a one-time compliance exercise [20]. The Working Group's 2022 companion report on implementing the UNGPs' "third pillar" — access to remedy — through transitional-justice mechanisms further signals that international expectations for corporate conduct in conflict zones are hardening from voluntary aspiration toward examinable obligation [22]. This normative architecture is reinforced at the domestic level by binding instruments such as the French Duty of Vigilance Law, Germany's Act on Corporate Due Diligence Obligations in Supply Chains, Norway's Transparency Act, and the European Union's Corporate Sustainability Due Diligence Directive, all of which convert what was once reputational risk management into enforceable legal duty [23]. Ruggie's foundational "Protect, Respect and Remedy" framework, from which the UNGPs derive, remains the conceptual bridge between international human rights law — traditionally binding only on states — and the operational reality that transnational corporations now wield state-like influence over conflict outcomes [24].

2.3 Export Control and Dual-Use Technology Governance

A third strand of relevant literature concerns the legal architecture that already constrains corporate "neutrality" from outside the firm: export control law. The United States regulates dual-use exports through two parallel regimes — the International Traffic in Arms Regulations (ITAR), administered by the State Department's Directorate of Defense Trade Controls, and the Export Administration Regulations (EAR), administered by the Commerce Department's Bureau of Industry and Security (BIS) [25,26]. The distinction matters ethically as well as legally: ITAR governs items with unambiguous military application, while EAR governs the far larger and more ambiguous category of dual-use goods — semiconductors, encryption software, certain categories of drones — whose civilian and military uses are inseparable at the point of sale [8,27]. A 2006 U.S. Government Accountability Office review found that BIS's licensing apparatus struggled even then to keep pace with the diversification of dual-use trade, a challenge that has only intensified with the proliferation of artificial intelligence, quantum computing, and space technologies as the new frontier of dual-use concern [27,28].

The Center for a New American Security (CNAS) frames the resulting governance dilemma succinctly: because critical technologies are now overwhelmingly developed in the commercial sector rather than through state-funded military research, "the United States needs the expertise of the private sector to adequately identify and prioritize critical technologies for regulation" [28]. This reverses the traditional relationship between state and firm in matters of security:

rather than the state directing a captive defence-industrial base, the state must now negotiate access to and control over infrastructure that private firms built for entirely civilian purposes. SIPRI's comparative work on dual-use export controls documents the proliferation of multilateral regimes attempting to manage this shift, including the Wassenaar Arrangement, the Missile Technology Control Regime, the Nuclear Suppliers Group, and the EU's Dual-Use Regulation, while noting that enforcement remains uneven across the 42 Wassenaar member states and that national implementation — such as Spain's extended brokering controls relative to France's narrower regime — varies considerably even within blocs ostensibly committed to a common standard [9,29,30]. Legal analysts further note that export controls, unlike financial sanctions, attach to the product or technology itself rather than to the nationality of the transacting party, giving them extraterritorial reach that can place a firm in violation of U.S. law even for a transaction between two non-U.S. entities involving U.S.-origin technology [26].

2.4 Historical Precedent: Corporate Disengagement from Apartheid South Africa

The clearest historical antecedent to the 2022 corporate exodus from Russia is the international divestment movement against apartheid South Africa, and the literature on that episode offers cautionary lessons for the present case. In 1977, the Reverend Leon Sullivan, then a board member of General Motors, issued a voluntary code — the Sullivan Principles — requiring signatory firms operating in South Africa to desegregate workplaces, extend equal pay for equal work, and invest in training programmes to advance Black South Africans into supervisory and management roles [31,32]. By the mid-1980s, coalitions including the American Committee on Africa, TransAfrica, and major religious bodies such as the National Council of Churches had transformed the Sullivan Principles from a voluntary corporate initiative into the benchmark against which institutional investors such as TIAA-CREF — then the largest private pension fund in the United States — pressured signatory firms to comply or divest [33,34]. Historical analysis by Sidorenko documents that the Principles were themselves the object of sustained internal criticism: Black trade unionists in South Africa dismissed them as a "toothless package" that improved individual working conditions without challenging the political architecture of apartheid itself, and Sullivan eventually abandoned incrementalism in 1987 to call for comprehensive economic sanctions and full corporate withdrawal [35,36]. Cambridge University Press's historical treatment of the episode similarly cautions against reading the Sullivan Principles as either a corporate "sellout" or a corporate triumph, showing instead how Black and white executives negotiated the limits of what corporate power could and could not achieve absent coordinated state action [32].

This precedent is instructive for the contemporary literature in at least three respects. First, it demonstrates that voluntary corporate codes of conduct in politically fraught environments tend to converge toward the lowest standard that preserves market access, unless reinforced by external pressure from investors, regulators, or civil society — a dynamic later echoed in the Yale CELI team's finding that many firms which pledged a "clean break" from Russia in 2022 had, within eighteen months, quietly resumed or maintained partial operations [37]. Second, it shows that full corporate withdrawal, once achieved, does not automatically translate into the desired political outcome, and can itself carry humanitarian costs for local employees that must be weighed against the political message the withdrawal sends [38]. Third, and most relevant to the present study, it establishes that "neutrality" was never seriously entertained as an option

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
Vol. 3, Issue 10, April 2026
Available Online : https://shodhprakashan.in/

by activists, investors, or ultimately by the firms themselves: the debate was never whether corporations would take a position, but which position, articulated through what mechanism, and enforced by whom.

3. Conceptual Framework: The Corporate Neutrality Spectrum

Building on the literature reviewed above, this paper proposes a two-dimensional analytical framework — the *Corporate Neutrality Spectrum* — for classifying corporate conduct in situations where a firm's products or services carry strategic consequence for an ongoing or anticipated armed conflict.

The horizontal axis captures the **degree of voluntary alignment** with a state security objective, ranging from strict commercial neutrality (continuing to serve all lawful customers regardless of the conflict) through selective disengagement (withdrawing from one party without actively supporting the other) to active alignment (materially supporting one belligerent's military or civilian resilience). The vertical axis captures the **depth of human-rights and conflict-sensitivity due diligence** performed before and during the decision, ranging from reactive, public-relations-driven responses to systematic, heightened due diligence of the kind envisioned by the UN Working Group's guidance [20].

Four illustrative quadrants emerge:

- **Quadrant I — Deliberated Alignment.** High due diligence, high alignment. A firm conducts a documented, conflict-sensitive assessment and then knowingly and transparently aligns its services with one party, accepting the reputational, legal, and human costs of that choice. Microsoft's documented decision to share cyber-threat intelligence with Ukrainian authorities, accompanied by public reasoning grounded in the illegality of the invasion under international law, approximates this quadrant [5].
- **Quadrant II — Reactive Alignment.** Low due diligence, high alignment. A firm withdraws or aligns rapidly under reputational or activist pressure without a systematic assessment of downstream humanitarian consequences — for example, employee welfare in the country of departure. Analysts describing the 2022 corporate exodus from Russia identified successive waves of departure driven respectively by principle, by fear of boycott, and finally by fear of being "identified as being on the wrong side of history," a sequence that suggests due diligence deepened only after the initial reactive wave [39].
- **Quadrant III — Passive Neutrality.** Low due diligence, low alignment. A firm continues business as usual, treating the conflict as commercially irrelevant, typically because it lacks the market exposure, product relevance, or stakeholder pressure to prompt reassessment. This quadrant is increasingly rare for firms with any dual-use exposure, and the ESG investment debate discussed in Section 5.3 shows that even historically "neutral" sectors such as institutional asset management are being forced out of this quadrant [40].
- **Quadrant IV — Deliberated Restraint.** High due diligence, low alignment. A firm conducts systematic risk assessment and deliberately declines to take an action that would escalate the conflict, even at the cost of appearing to favour the aggressor. Musk's decision to withhold Starlink activation over Crimea in September 2022, reportedly motivated by fear of triggering nuclear escalation, is the paradigmatic — and most contested — example

of this quadrant, precisely because "restraint" toward an aggressor state's territorial claims is difficult to distinguish, from the victim state's perspective, from complicity [7,41].

The framework's central analytical claim is that Quadrant III — genuine passive neutrality — becomes structurally unstable once a firm's product acquires strategic utility. Firms are pushed, by market pressure, activist campaigns, government regulation, or the sheer operational logic of their own infrastructure, toward one of the other three quadrants. The ethically salient question this paper pursues, therefore, is not how firms can remain in Quadrant III, but how the movement between quadrants can be made more accountable, more transparent, and more consonant with international humanitarian and human rights norms.

4. Methodology

This paper adopts a qualitative, document-based case-study methodology, appropriate to a normative and interpretive research question that cannot be resolved through experimental or purely quantitative means. Four cases were purposively selected for their capacity to illuminate distinct dimensions of the corporate-neutrality problem: (i) the mass corporate withdrawal from Russia following the 2022 invasion of Ukraine, selected for its unprecedented scale and its generation of a publicly documented dataset (the Yale CELI list); (ii) the Starlink controversy, selected because it isolates the tension between commercial infrastructure and battlefield consequence in its starkest form, with decision-making concentrated in a single identifiable executive; (iii) the treatment of defence-sector securities within ESG investment frameworks, selected because it demonstrates how the neutrality question propagates from operating companies to the capital markets that finance them; and (iv) the export-control regime, selected because it represents the external, state-imposed boundary within which any claim to corporate discretion must operate.

Primary and secondary sources were drawn from peer-reviewed business-ethics journals, United Nations and OHCHR policy documents, SIPRI research publications, contemporaneous reporting from established news organisations (Reuters-sourced wire reporting via Axios, TechCrunch, Euronews, and CNN Business), Yale School of Management institutional publications, and specialist financial and legal commentary (Global Investigations Review, Wealthbriefing, and sector ESG analyses). Data were triangulated across at least two independent sources wherever a specific figure or claim was load-bearing for the analysis, consistent with standard practice in qualitative case-study research. The analysis is interpretive rather than causal: it does not claim to establish that any single firm's decision was ethically optimal, but rather uses the empirical record to test the explanatory adequacy of the Corporate Neutrality Spectrum developed in Section 3.

5. Case Studies

5.1 The 2022 Corporate Exodus from Russia

The corporate response to Russia's February 2022 invasion of Ukraine constitutes the largest coordinated private-sector withdrawal from a national market in modern economic history. Tracking work led by Yale School of Management professor Jeffrey Sonnenfeld and the Yale

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
Vol. 3, Issue 10, April 2026
Available Online : https://shodhprakashan.in/

Chief Executive Leadership Institute (CELI) began with a list of fewer than 100 companies in the invasion's first week and had documented withdrawal announcements from more than 400 companies within three weeks, over 1,000 within eight months, and had graded over 1,000 firms on a letter-grade scale (A through F) reflecting the completeness of their disengagement by mid-2023 [2,3,42]. Analysts at Axios characterised the exodus as unfolding in three discernible waves: an initial group of "first movers" driven by moral principle and internal employee pressure; a second group responding to financial-market signals and consumer boycott threats; and a third group motivated primarily by reputational fear of being remembered as having sided with the aggressor [39].

Within the technology sector specifically, the pattern of withdrawal was rapid but uneven in scope. Apple halted all physical product sales, restricted access to Apple Pay and other digital services, and removed RT and Sputnik from its App Store globally, while separately disabling live traffic and incident-reporting features in Ukraine's Apple Maps as a protective measure against their exploitation for targeting [1]. Microsoft suspended new product and service sales in Russia, removed RT applications from its store, de-ranked Kremlin-aligned outlets in Bing search results, and — in a step with direct security consequences — disclosed that it had detected "offensive and destructive" cyberattacks against Ukrainian digital infrastructure on the first day of the invasion and had since provided Ukrainian officials with threat intelligence and defensive guidance [4,5]. Google paused advertising sales in Russia, suspended live Google Maps data in areas at risk of Russian targeting, and added information on refugee and migrant assistance centres to its mapping products [43,44]. Cloud infrastructure providers — Amazon Web Services, Microsoft Azure, Google Cloud, and IBM — each suspended new sales in Russia, with Amazon noting it had no data centres in Russia and, as a matter of standing policy, did not conduct business with the Russian government even prior to the invasion [45].

Not every announced withdrawal proved permanent or complete. A July 2023 CNN Business investigation, drawing on continued Yale CELI monitoring, found that companies including Heineken, Unilever, and Mondelez — initially awarded Yale's highest "A" grade for a "clean break" — retained substantial operations, employees, and even launched new product lines in Russia sixteen months after their public withdrawal pledges [37]. This finding is directly relevant to the Corporate Neutrality Spectrum developed in Section 3: firms that appeared, in the initial reactive wave (Quadrant II), to have moved decisively toward alignment with Ukraine and its allies in fact reverted, in practice, toward a form of disguised Quadrant III passivity once acute reputational pressure subsided — a pattern strikingly consistent with the Sullivan Principles-era finding that voluntary corporate commitments tend to regress toward the minimum standard compatible with continued market access absent sustained external enforcement [35].

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
Vol. 3, Issue 10, April 2026
Available Online : https://shodhprakashan.in/

Table 1. Selected Technology-Sector Corporate Responses to the 2022 Russian Invasion of Ukraine

Company	Primary Action Taken	Security-Relevant Dimension	Approximate Timing
Microsoft	Suspended new sales; removed RT from app store; shared cyber-threat intelligence with Ukraine	Direct defensive cyber-support to a belligerent state	28 Feb–4 Mar 2022 [4,5]
Apple	Halted product sales; restricted Apple Pay; disabled live Ukraine Maps traffic data	Withheld data exploitable for military targeting	Late Feb–Mar 2022 [1]
Google/Alphabet	Paused ad sales; suspended live Maps data in Ukraine; added refugee-centre information	Denial-of-data to reduce targeting risk; humanitarian information provision	Late Feb–Mar 2022 [43,44]
Amazon/AWS	Suspended new sales in Russia; confirmed no Russian data centres	Passive market exit; no direct combat-relevant support disclosed	Mar 2022 [45]
SpaceX (Starlink)	Activated satellite terminals for Ukraine; later restricted use over Crimea	Direct provision of battlefield communications infrastructure	Feb 2022 onward [6,7,41]
Oracle	Suspended all Russian operations	Passive market exit	2 Mar 2022 [46]

Source: compiled by the author from Euronews, TechCrunch, Courthouse News, PBS, and CEPA reporting cited above.

5.2 Starlink: Commercial Infrastructure as Battlefield Infrastructure

The Starlink case isolates the corporate-neutrality dilemma in its purest form because decision-making authority over a system of demonstrable strategic consequence rested, for an extended period, with a single private individual rather than a diffuse corporate bureaucracy or an elected government. Following Russia's invasion, Ukraine's military came to rely on Starlink terminals for frontline communication, drone-strike coordination, and artillery targeting to an extent that analysts described as difficult to substitute given the absence of any comparable alternative network [47,48]. This dependence gave SpaceX's leadership a form of *de facto* battlefield veto power unprecedented for a private commercial contractor.

The controversy crystallised in September 2022, when — according to excerpts from a biography of Musk published by *The Washington Post* — Ukrainian forces requested Starlink activation over Crimean waters near Sevastopol to support a planned strike on the Russian Black Sea Fleet, and Musk declined the request, citing fear that facilitating the attack would make SpaceX "explicitly complicit in a major act of war and conflict escalation," given the risk

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
Vol. 3, Issue 10, April 2026
Available Online : https://shodhprakashan.in/

of a Russian nuclear response to an assault on Crimea [41,49]. The refusal prompted a formal letter from U.S. Senators Elizabeth Warren, Jeanne Shaheen, and Tammy Duckworth to the Secretary of Defense, questioning whether a private contractor should retain unilateral authority to override an ally's military operations and noting that SpaceX functioned as "a prime contractor and a critical industry partner" for the Department of Defense [50]. Air Force Secretary Frank Kendall later confirmed that the episode had prompted the Pentagon to reconsider how explicitly future contracts must specify the permitted military uses of commercially procured space services [48].

The dilemma recurred in subsequent years as reports emerged that Russian forces had themselves obtained and were using Starlink terminals via parallel importation networks, despite SpaceX's public statements that it does not sell or knowingly support Russian government or military use of the service [51,52]. SpaceX president Gwynne Shotwell further stated in February 2023 that Ukraine had "weaponized" Starlink in ways beyond the terms of its intended humanitarian use, and that the company had taken unspecified action to constrain Ukrainian military applications of the network — remarks that Ukrainian officials received with what press accounts described as puzzlement and anger, given the network's acknowledged centrality to Ukraine's survival [53]. By 2025–2026, the Pentagon and allied governments including Poland — which alone pays approximately $50 million annually to sustain Starlink service in Ukraine — had moved to formalise and subsidise the arrangement, converting what began as a personal, ad hoc corporate decision into a semi-institutionalised element of allied defence procurement [6].

The Starlink episode demonstrates, more starkly than any other case examined in this paper, that Quadrant IV "deliberated restraint" is not ethically neutral simply because it withholds escalation. Restraint that has the practical effect of protecting an aggressor's military assets is a substantive strategic choice, regardless of the private motivations — nuclear-escalation anxiety, corporate liability concerns, or personal political sympathy — that inform it. Commentary from the Center for European Policy Analysis (CEPA) frames the underlying structural problem precisely: "Whatever the truth, Starlink's potential misuse raises serious concerns about Internet infrastructure, more and more of which are privately built and run" [47]. The episode also illustrates a governance vacuum: no existing international legal framework clearly allocates responsibility for battlefield decisions made by privately owned dual-use infrastructure operating with implicit but not always explicit state authorisation.

5.3 The Defence Sector and the ESG Investment Debate

The neutrality dilemma extends beyond operating companies into the capital markets that finance them, most visibly in the debate over whether defence and weapons-manufacturing securities belong in Environmental, Social and Governance (ESG) investment portfolios. Defence stocks have been excluded from mainstream ethical investment funds since the earliest such vehicles, including the UK's Stewardship funds launched by Friends Provident in 1984, on the premise that arms manufacturing is categorically incompatible with the "S" (social) pillar of ESG analysis [54]. Russia's 2022 invasion of Ukraine reopened this settled question with unusual force. UK government ministers publicly characterised the exclusion of defence firms from ESG-labelled funds as "perverse" given the sector's role in collective security, and

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
Vol. 3, Issue 10, April 2026
Available Online : https://shodhprakashan.in/

convened meetings between major asset managers and defence contractors including BAE Systems and Leonardo to discuss capital access [40,55].

The resulting debate exposes a genuine and unresolved normative tension rather than a simple case of activist overreach or industry self-interest. Proponents of continued exclusion, such as Candriam's global head of responsible investment, argue that weapons manufacturing remains definitionally incompatible with sustainable investment principles regardless of the geopolitical justification offered for any particular conflict, and that decisions about a state's appropriate level of military resilience "should not be up to investors to decide, certainly not sustainable investors" [56]. A parallel critique from the Don't Bank on the Bomb research network argues that framing ESG exclusions as financially "starving" the defence industry is empirically unsupported, since major European contractors such as Thales and Leonardo — both excluded by several institutional investors specifically for their nuclear-weapons-related activities — have continued to report record profits even amid continued exclusion, suggesting that access to public capital markets and access to private defence-procurement revenue are not, in practice, equivalent [57]. Financial advisory firm Parmenion further observes that the debate cannot be cleanly resolved by restricting eligible defence investment to firms domiciled in NATO countries, since NATO-domiciled defence contractors have, according to Parmenion's summary of UN Human Rights Council findings, also supplied the totality of arms transferred to Israel, a case in which the same Council found "clear evidence" of law-of-war violations in Gaza — meaning the geographic or alliance-based proxy for "acceptable" versus "unacceptable" defence investment breaks down under closer scrutiny [40].

At the same time, industry-side analysts note a genuine softening of the categorical exclusion norm, with a growing number of ESG strategies re-engaging cautiously with adjacent sub-sectors such as cybersecurity, logistics, and defence infrastructure providers that fall short of direct weapons manufacture, on the theory that ESG integration is a risk-assessment methodology rather than an inherently moral judgment, and that blanket exclusion conflates the two [54,58]. This shift illustrates, in miniature, the same movement away from Quadrant III passivity documented in the operating-company cases above: institutional investors that once treated "no defence exposure" as an adequate neutrality position are increasingly required to articulate an affirmative, documented rationale for either inclusion or exclusion, a due-diligence burden that maps directly onto the vertical axis of the Corporate Neutrality Spectrum.

Table 2. Comparative Positions in the Defence-Sector ESG Debate

Stakeholder Position	Core Argument	Representative Source
Continued categorical exclusion	Weapons production is inherently incompatible with sustainability criteria; investors lack visibility into end-use and cannot ensure arms do not reach abusive actors	Candriam [56]; Parmenion [40]
Selective re-engagement	ESG is a risk-methodology, not an ethical litmus test; adjacent defence sub-sectors	Lloyds Bank / Trustnet analysis [54]; ILIM [58]

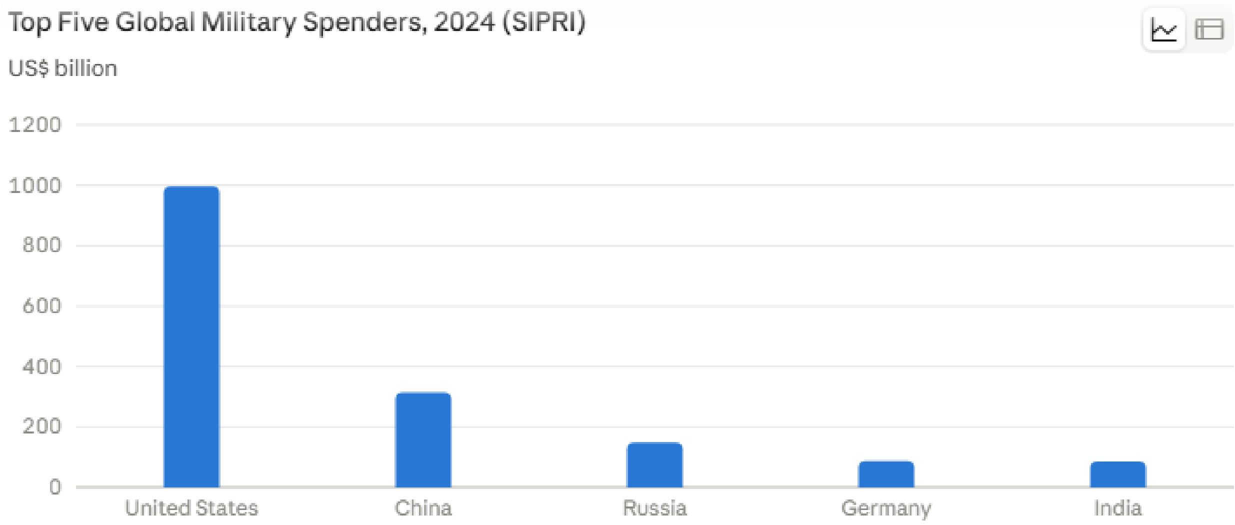
	(cyber, logistics) may meet ESG criteria with clearer regulation	
Full sector re-inclusion	National security is itself a social good; categorical exclusion undermines collective defence capacity at a moment of acute geopolitical risk	UK government ministers, cited in Parmenion [40] and *interactive investor* [55]
Empirical skepticism of the "capital starvation" claim	Record defence-sector profits during the exclusion period suggest ESG exclusion has not materially constrained the industry's access to capital	Don't Bank on the Bomb [57]

5.4 Export Control as an External Constraint on Corporate Discretion

The three cases above concern voluntary corporate choice; the fourth case concerns the legal architecture that removes choice altogether once a transaction is classified as controlled. U.S. export-control law divides jurisdiction between the State Department's ITAR regime, governing unambiguously military articles, and the Commerce Department's EAR regime, governing dual-use goods [25,26]. The distinction between export controls and financial sanctions is legally consequential: sanctions generally attach to the identity of the transacting party, while export controls attach to the product or technology itself and apply extraterritorially to any transaction involving U.S.-origin technology, regardless of whether a U.S. person is party to it [26]. A company developing an ostensibly civilian product — Wiley's legal analysis cites the illustrative example of autonomous maritime drones marketed for environmental mapping — can nonetheless be captured by dual-use rules if the underlying technology is adaptable to naval surveillance or mine detection, regardless of the firm's stated commercial intent [10]. Firms seeking to do classified work or access Controlled Unclassified Information must additionally satisfy Foreign Ownership, Control, or Influence (FOCI) mitigation requirements — a process that can take years and requires governance mechanisms such as information firewalls and proxy board structures [10].

This legal architecture matters for the neutrality question because it demonstrates that, for an important category of technologies, the state has already pre-empted the firm's discretion to claim neutrality: possession or transfer of certain dual-use goods is, by statute, a foreign-policy act regardless of the firm's professed intent. The GAO's 2006 review found that the Commerce Department's Bureau of Industry and Security struggled even in the pre-9/11-legacy period to maintain an accurate and current picture of which end-users and applications posed diversion risk, drawing on watchlists spanning the Denied Persons List, the Unverified List, and equivalent State Department and Homeland Security instruments [11]. SIPRI's comparative research documents the resulting patchwork of multilateral regimes — the Wassenaar Arrangement (42 member states), the Missile Technology Control Regime, the Nuclear Suppliers Group, the Australia Group, and UN Security Council Resolution 1540 — each attempting, with only partial success, to harmonise dual-use controls across jurisdictions with materially different risk tolerances and enforcement capacity [9,29].

ISSN : 2583-9861
Vol. 3, Issue 10, April 2026
Available Online : https://shodhprakashan.in/



Top Five Global Military Spenders, 2024 (SIPRI)

Category	Military Expenditure 2024 (US$ billion)
United States	997
China	314
Russia	149
Germany	88.5
India	86.1

6. Data Analysis and Results

Synthesising the four case studies produces several patterns that bear directly on the Corporate Neutrality Spectrum introduced in Section 3.

First, scale and speed of alignment correlate strongly with public visibility and activist mobilisation rather than with the objective security relevance of the firm's product. The Yale CELI dataset shows that the number of tracked companies grew from under 100 to over 1,000 within roughly six months of the invasion [2,3], a growth curve that tracks media and activist attention far more closely than any independent measure of each firm's strategic importance to the Russian war effort. Firms with genuinely dual-use, security-relevant products — cloud infrastructure, satellite communications, cybersecurity services — moved early and were joined subsequently by firms (fast-food franchises, beverage companies, consumer retailers) whose exit had primarily symbolic and economic-pressure value rather than direct security consequence [37,45].

Second, the depth of due diligence performed varied inversely with the speed of the initial decision. Microsoft's simultaneous disclosure of detected cyberattacks and provision of defensive intelligence to Ukrainian officials suggests an internal decision architecture capable of rapid, security-literate assessment — arguably approximating Quadrant I ("deliberated alignment") [5]. By contrast, the pattern of companies later found by Yale researchers to have

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
Vol. 3, Issue 10, April 2026
Available Online : https://shodhprakashan.in/

quietly walked back "clean break" pledges — Heineken, Unilever, Mondelez — is more consistent with Quadrant II ("reactive alignment"), in which an initial public commitment outpaced the firm's actual operational and reputational risk tolerance [37].

Third, the global military-spending environment against which these corporate decisions unfold has itself shifted structurally, raising the stakes of any individual firm's positioning. SIPRI's 2024 data show that global military expenditure reached an all-time high of US$2.718 trillion, a 9.4 percent real-terms increase over 2023 and the sharpest single-year rise since 1988 [59,60]. The five largest spenders — the United States, China, Russia, Germany, and India — together accounted for 60 percent of global military spending, with the United States alone responsible for 37 percent of the world total [59,61]. Ukraine's own military expenditure, at US$64.7 billion, represented 34 percent of its GDP, the highest military burden recorded by any state in the SIPRI dataset for that year, while Russia's expenditure rose 38 percent to US$149 billion, or 7.1 percent of its GDP [62,63].

Table 3. Global Military Expenditure, Top Spenders, 2024 (SIPRI data)

Rank	Country	Expenditure (US$ billion)	Change vs 2023	% of GDP
1	United States	997	+5.7%	~3.4%
2	China	314	n/a	n/a
3	Russia	149	+38%	7.1%
4	Germany	88.5	+28%	n/a
5	India	86.1	n/a	n/a
—	Ukraine	64.7	+2.9%	34.0% (highest globally)

Source: SIPRI Trends in World Military Expenditure, 2024, as reported by Euro-SD, Tribune India, and Babel.ua [59,61,62,63].

The chart above visualises the concentration of global military spending among a small number of states — precisely the environment in which a handful of dual-use technology firms headquartered predominantly in those same states now find themselves making consequential wartime decisions. This concentration is analytically important: it means that the "national security" pole of the corporate-neutrality dilemma is not diffuse across the international system but is disproportionately exercised through the regulatory and diplomatic leverage of a small set of governments — chiefly the United States — whose export-control and sanctions regimes (Section 5.4) already constrain the discretion of firms domiciled or transacting within their jurisdiction.

Fourth, the ESG investment debate (Section 5.3) demonstrates that the neutrality question is propagating "upstream" from operating companies to asset owners and managers, who face an analogous but distinct version of the dilemma: whether continued exclusion of the defence sector from sustainable investment vehicles constitutes principled neutrality or, alternatively, a form of free-riding on the collective security that defence spending provides. The empirical claim that record defence-sector profits persist despite ESG exclusion [57] suggests that, at least for large-capitalisation defence contractors, the exclusion functions more as a reputational

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
Vol. 3, Issue 10, April 2026
Available Online : https://shodhprakashan.in/

and moral positioning exercise for asset managers than as an effective capital constraint on the sector — a finding that itself carries normative weight, since it implies that continued exclusion imposes primarily symbolic rather than substantive costs, weakening the "national security requires ESG inclusion" argument advanced by some European officials [40].

7. Discussion: Competing Perspectives

7.1 The Shareholder-Primacy Perspective

From a strict Friedmanite standpoint, the wave of 2022 corporate withdrawals from Russia is defensible primarily to the extent that it served shareholder interests — whether through avoidance of sanctions-related legal liability, protection of brand equity in larger and more lucrative Western markets, or pre-emption of consumer boycotts [64]. Under this reading, Digital Trends' technology-industry analysis is instructive: technology analyst Rob Enderle attributed the Russia exodus primarily to "brand protection and liability protection" rather than to a freestanding moral commitment, noting that companies "were being called out, and people were boycotting them for not leaving Russia, and sanctions could have put their assets at risk" [65]. On this view, the language of moral commitment that accompanied many corporate announcements is best understood as instrumental communication directed at shareholders and consumers rather than as evidence of an independent ethical judgment by the firm. This perspective, while frequently dismissed as cynical, retains genuine explanatory power: it correctly predicts the subsequent finding that firms without equivalent market exposure or reputational vulnerability in the West — smaller Russia-dependent manufacturers, certain professional-services firms — were markedly slower to exit, and that several nominally departed firms quietly retained partial operations once acute public attention subsided [37]. A rigorous shareholder-primacy critique of corporate "moral" positioning in conflict zones would insist that boards disclose the actual risk-adjusted financial calculus behind withdrawal decisions rather than obscuring commercial self-interest behind humanitarian language — a transparency demand that, notably, converges with the stakeholder-theory demand for documented due diligence discussed below, even though the two frameworks begin from opposed first principles.

7.2 The Stakeholder and Human-Rights Perspective

The UNGP-grounded stakeholder perspective evaluates the same episodes by a different metric: not whether withdrawal served shareholder value, but whether the firm conducted and documented a conflict-sensitive human-rights assessment before acting, and whether it considered the interests of affected stakeholders beyond its immediate commercial counterparties [18,20]. Judged against this standard, the technology-sector responses examined in Section 5.1 score unevenly. Microsoft's simultaneous provision of cyber-defence support to Ukraine alongside its market withdrawal from Russia suggests an institutional capacity to integrate security and human-rights considerations into a single, relatively coherent decision architecture [5]. By contrast, firms that announced abrupt withdrawal without a documented assessment of the resulting harm to local employees — a concern explicitly raised, and explicitly set aside as insufficient justification for continued operation, by Yale's Sonnenfeld, who argued that "the idea is not to minimize the pain" but to recognise that economic pressure on the Russian population was itself a deliberate and necessary instrument of the broader sanctions strategy [66] — illustrate the genuine ethical cost that even a "correct" alignment decision can impose on stakeholders who bear no responsibility for the conflict. The UN Working Group's heightened-due-diligence guidance would require such firms to document, not merely announce, their assessment of these trade-offs — a standard that, on the available public record, few firms in the 2022 cohort appear to have met with full transparency [20,21].

7.3 The National Security and State-Centric Perspective

From the standpoint of the state — articulated most clearly by the export-control and defence-procurement literatures reviewed in Sections 2.3 and 5.4 — the relevant ethical question is not what corporations owe to abstract global stakeholders, but what obligations attach to firms whose technology has become load-bearing for an allied state's territorial defence. This perspective treats the Starlink episode as the paradigm case: from Kyiv's vantage point, Musk's September 2022 refusal to enable a strike near Sevastopol was not a neutral act of restraint but a unilateral veto over an ally's legitimate military operation, exercised by an actor accountable to no electorate and bound by no treaty obligation [41,50]. The bipartisan Senate inquiry into the episode reflects this state-centric concern precisely: the senators' letter did not ask whether Musk's decision was ethically defensible in the abstract, but whether a private contractor should retain such authority at all, given SpaceX's simultaneous status as "a prime contractor and a critical industry partner" for the U.S. Department of Defense [50]. Air Force Secretary Kendall's subsequent statement that future contracts must more explicitly specify permitted military uses reflects an institutional response consistent with this perspective: rather than relying on the goodwill or personal judgment of corporate leadership, the state seeks to convert what was previously an area of corporate discretion into a matter of binding contractual and, ultimately, regulatory obligation [48]. Extended to its logical conclusion, this perspective implies that dual-use infrastructure of sufficient strategic consequence should not remain within the unconstrained discretion of private actors at all — a position with significant implications for the future governance of commercial space, cloud, and satellite-communications infrastructure.

7.4 The Just War and Neutrality-Theory Perspective

Classical Just War theory, developed originally to constrain the conduct of states, offers a less commonly applied but analytically productive lens for evaluating corporate conduct in conflict. Traditional principles of jus in bello — discrimination between combatants and non-combatants, and proportionality of harm to military advantage — translate imperfectly but usefully to the corporate context. A firm's decision to withhold or provide targeting-relevant data (as in Apple's suspension of live Ukraine Maps traffic information [1], or the hypothetical Starlink-enabled strike on Sevastopol [41]) implicates discrimination and proportionality concerns even though the firm itself fires no weapon. Historical neutrality doctrine, most fully elaborated in the law and practice of permanently neutral states such as Switzerland, holds that genuine neutrality requires impartiality applied *equally* to all belligerents, not selective withdrawal from one party while implicitly favouring another through continued service, technology transfer, or market access. Measured against this classical standard, none of the firms examined in this paper's case studies achieved neutrality in the strict sense: each made choices — whether to withdraw, whether to provide cyber-defence assistance, whether to activate or restrict satellite service — that had asymmetric effects on the two belligerents. This finding directly supports the paper's central thesis: what firms describe, and what the public frequently accepts, as "neutral" corporate conduct in modern warfare is, on close inspection, almost never neutral in the classical sense; it is instead a form of selective, often reactive, alignment dressed in the rhetoric of non-involvement.

7.5 Synthesis: Toward a Conditional Neutrality Standard

Reconciling these four perspectives does not require abandoning the concept of corporate neutrality altogether, but it does require redefining what a defensible neutrality claim can plausibly mean for a firm whose products carry dual-use, conflict-relevant capability. This paper proposes a *conditional neutrality standard*, synthesising elements of all four perspectives examined above: a firm may legitimately claim ethical neutrality only where (i) it has conducted and documented heightened human-rights and conflict-sensitivity due diligence consistent with UN Working Group guidance [20]; (ii) any resulting alignment decision is disclosed with its underlying rationale rather than obscured behind generic humanitarian language, satisfying the shareholder-primacy demand for transparency [65]; (iii) the decision accounts for proportionality and discrimination consistent with Just War principles, particularly regarding data or infrastructure with direct targeting relevance [41]; and (iv) the firm accepts external, ideally state- or treaty-based, accountability for decisions that carry battlefield consequence, rather than retaining unilateral and unreviewable discretion, addressing the state-centric concern raised by the Starlink case [50]. Under this standard, "neutrality" is redefined from an empirical claim about non-involvement — which the evidence in this paper suggests is rarely achievable — to a normative claim about the integrity, transparency, and accountability of the process by which involvement is decided.

8. Policy Implications

For **firms**, the analysis suggests three concrete governance reforms. First, boards should establish standing conflict-risk committees, analogous to existing audit or cybersecurity committees, tasked specifically with heightened human-rights due diligence for operations in or adjacent to active or anticipated conflict zones, consistent with the UN Working Group's guidance [20,21]. Second, firms whose products carry demonstrable dual-use or targeting-relevant capability should pre-establish, in consultation with relevant government counterparties, clear protocols for wartime service provision or restriction, reducing reliance on ad hoc, individually discretionary decisions of the kind that generated the Starlink controversy [48,50]. Third, firms should resist the temptation identified in the Sullivan Principles and 2022 Russia-exodus literature to announce maximal public commitments under acute reputational pressure that are not subsequently sustained, since the credibility cost of a documented reversal — as Yale researchers found with Heineken, Unilever, and Mondelez — exceeds the reputational benefit of the original announcement [35,37].

For **investors and asset managers**, the ESG defence-sector debate (Section 5.3) suggests that categorical exclusion policies should be replaced with documented, criteria-based screening that distinguishes between weapons categories (for example, controversial or indiscriminate

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
Vol. 3, Issue 10, April 2026
Available Online : https://shodhprakashan.in/

weapons systems, per existing frameworks such as those applied to cluster munitions and nuclear-weapons-adjacent activity) and defence-adjacent infrastructure whose exclusion serves primarily symbolic rather than substantive ends [56,58]. Given the empirical finding that ESG exclusion has not materially constrained large defence contractors' profitability [57], asset managers should be transparent with beneficiaries about which function — capital allocation or moral positioning — their exclusion policy is actually performing.

For **states and regulators**, the export-control literature and the Starlink case together point toward the need for clearer, ex ante contractual and regulatory frameworks governing the wartime obligations of dual-use infrastructure providers, rather than relying on post hoc congressional inquiry after a controversial decision has already been made [10,48,50]. The GAO's long-standing critique of BIS's dual-use licensing capacity [11] suggests that regulatory modernisation — particularly for emerging categories such as commercial satellite constellations, cloud AI infrastructure, and autonomous systems — remains overdue relative to the pace of dual-use technology diffusion documented by CNAS [28]. Multilateral coordination through existing regimes such as the Wassenaar Arrangement should be extended explicitly to cover commercial space and cloud infrastructure, categories that did not exist in their current strategically consequential form when most of these regimes were originally designed [9,29].

9. Limitations

This study is subject to several limitations that qualify its conclusions. First, the case-study methodology relies substantially on public corporate statements, journalistic reporting, and institutional tracking projects (notably the Yale CELI dataset), which are themselves subject to incentives toward favourable self-presentation on the part of the firms being tracked; internal corporate decision-making processes remain largely opaque to external researchers, limiting the paper's ability to verify claimed due-diligence processes against actual internal deliberation. Second, the analysis focuses predominantly on firms headquartered in the United States and allied Western states; the conduct of firms headquartered in China, India, and other states that maintained commercial relationships with Russia throughout the conflict was outside this paper's scope but would substantially enrich a comparative analysis of how "neutrality" claims are constructed differently across political and regulatory contexts. Third, the SIPRI military-expenditure data and Yale CELI classifications, while authoritative, are themselves contested by the actors they describe and subject to revision; figures cited reflect the most recent published datasets available at the time of writing and should be understood as provisional rather than final. Finally, this paper's normative framework — the Corporate Neutrality Spectrum and the conditional neutrality standard derived from it — represents one plausible synthesis of the four perspectives examined, not a claim to have resolved the underlying ethical disagreement between shareholder-primacy, stakeholder, state-centric, and Just War approaches, which reflect genuinely competing value commitments rather than a single latent consensus awaiting discovery.

SHODH PRAKASHAN
An International Open Access, Peer Reviewed, Refereed Journal
ISSN : 2583-9861
Vol. 3, Issue 10, April 2026
Available Online : https://shodhprakashan.in/

10. Conclusion

The premise that corporations can remain neutral bystanders to armed conflict has not survived contact with the realities of twenty-first-century warfare, in which cloud infrastructure, satellite communications, and digital platforms are frequently as strategically consequential as conventional military assets. The case studies examined in this paper — the unprecedented corporate exodus from Russia following the 2022 invasion of Ukraine, the singular governance anomaly of Starlink's battlefield role, the unresolved debate over defence-sector inclusion in ESG investment frameworks, and the pre-existing legal architecture of export controls — collectively demonstrate that firms possessing dual-use, conflict-relevant capability face a structural incapacity to remain in what this paper terms Quadrant III passive neutrality. The meaningful ethical and policy question, therefore, is not whether corporations will take sides in modern warfare, but through what governance processes, with what transparency, and subject to what external accountability those choices will be made. The conditional neutrality standard proposed in Section 7.5 — requiring documented heightened due diligence, transparent disclosure of underlying rationale, adherence to discrimination and proportionality principles, and acceptance of external accountability — offers one path toward reconciling the competing demands of shareholder-primacy, stakeholder, state-centric, and Just War perspectives, without pretending that a return to genuine, classical neutrality remains available to firms whose infrastructure has become, whether by design or by circumstance, an instrument of war. Future research should extend this analysis through firm-level interviews with corporate decision-makers, comparative study of non-Western corporate responses to the same conflicts, and longitudinal tracking of whether the governance reforms proposed here — standing conflict-risk committees, pre-negotiated wartime service protocols, and criteria-based rather than categorical ESG screening — are in fact adopted, and whether their adoption measurably improves the consistency between firms' public commitments and their documented conduct.

References

1. Euronews. Which tech companies are cutting ties with Russia over its war in Ukraine? Euronews Next. 2022 Mar 17.
2. Yale Daily News. SOM professor updates viral list of Russia-affiliated companies. New Haven: Yale Daily News; 2022 Mar 29.
3. Yale School of Management. Over 1,000 companies have curtailed operations in Russia—but some remain. New Haven: Yale SOM; 2025 Feb 24.
4. TechCrunch. Microsoft halts all new sales in Russia. San Francisco: TechCrunch; 2022 Mar 4.
5. PressReader. Microsoft kicks Russia Today off app store over 'tragic' invasion. Computeractive UK. 2022 Mar 16.
6. Euronews. Fact check: Is Elon Musk allowing Russia to use Starlink to attack Ukraine? Euronews. 2026 Feb 3.
7. Eurotopics.net. Ukraine: Musk blocks Starlink for Russian military. 2026 Feb 18.
8. United States Department of State, Bureau of Arms Control and Nonproliferation. Conventional Dual-Use Technology Controls. Washington (DC): US Department of State; 2025.

9. Stockholm International Peace Research Institute (SIPRI). Dual-use export controls. Stockholm: SIPRI; 2025.
10. Wiley LLP. National security, legal readiness, and U.S. engagement for international dual-use technology companies. Washington (DC): Wiley; 2025 Oct 3.
11. United States Government Accountability Office. Export Controls: Improvements to Commerce's Dual-Use System Needed to Ensure Protection of U.S. Interests in the Post-9/11 Environment. Washington (DC): GAO; Report No. GAO-06-638.
12. Friedman M. The social responsibility of business is to increase its profits. New York Times Magazine. 1970 Sep 13.
13. Hühn MP. Business ethics: Between Friedman and Freeman? A response to A Puzzle about Business Ethics. Business Ethics, the Environment & Responsibility. 2023.
14. Ferrero I, Sison AJG. Must Milton Friedman embrace stakeholder theory? Business and Society Review. 2014.
15. Freeman RE. Strategic Management: A Stakeholder Approach. Boston: Pitman Publishing; 1984.
16. Pressbooks (SMC). Stakeholder theory, stockholder primacy laws and challenge to same. In: Business Ethics and Social Responsibility. Santa Monica College; 2023.
17. United Nations Office of the High Commissioner for Human Rights (OHCHR). Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework. Geneva: OHCHR; 2011.
18. OHCHR. What do the UN Guiding Principles on Business and Human Rights say about protecting and respecting human rights in conflict-affected contexts? Geneva: OHCHR.
19. Davis R. The UN Guiding Principles on Business and Human Rights and conflict-affected areas: state obligations and business responsibilities. International Review of the Red Cross. 2012.
20. United Nations Development Programme (UNDP), UN Working Group on Business and Human Rights. Heightened Human Rights Due Diligence for Business in Conflict-Affected Contexts: A Guide. New York: UNDP; 2022 Jun 16.
21. Business & Human Rights Resource Centre. UNDP and UN Working Group launch new guide on heightened human rights due diligence for business in conflict-affected contexts. 2022 Jun 22.
22. OHCHR. UN experts launch new guidance for businesses working in conflict-affected regions. Geneva: OHCHR; 2022 Jul 27.
23. Global NAPs (National Action Plans on Business and Human Rights). Mandatory human rights due diligence. 2024.
24. OHCHR. The business, human rights and conflict-affected regions project. Geneva: OHCHR.
25. Global Investigations Review. Spotlighting export controls in the United States. GIR: The Guide - Sanctions, 5th ed. 2024 Jun 20.
26. Descartes Systems Group. Dual-Use Exports. Waterloo: Descartes; 2024.
27. GAO-06-638. [See ref 11.]
28. Fitt J, et al. Dual-Use Technology and U.S. Export Controls. Washington (DC): Center for a New American Security (CNAS); 2023 Jun 9.
29. SIPRI. [See ref 9.]
30. Global Investigations Review. [See ref 25.]

31. Boston University Trustees Archive. The Sullivan Principles. Boston: BU; 1977 (rev. 1984).
32. Angelo AH. Black Power in the Boardroom: Corporate America, the Sullivan Principles, and the Anti-Apartheid Struggle. Enterprise & Society. Cambridge University Press.
33. Christian Science Monitor. Apartheid protests lead more US firms in South Africa to stress equal rights. Boston: CSM; 1986 Apr 1.
34. Michigan in the World (University of Michigan). Corporate Response: The Sullivan Principles. Ann Arbor: University of Michigan.
35. Sidorenko LV. The Sullivan Principles as a Way to Struggle Against the Apartheid Regime in South Africa. Africa Journal. 2024 Dec 28.
36. Angelo AH. [See ref 32.]
37. CNN Business. Heineken, Unilever and Oreo maker Mondelez accused of breaking promises to leave Russia. Atlanta: CNN; 2023 Jul 11.
38. Inquirer.com. A Yale professor's list of companies staying in Russia has put the business world on notice. Philadelphia: The Philadelphia Inquirer; 2022 Mar 8.
39. Axios. Over 300 companies have exited Russia since invasion. Washington (DC): Axios; 2022 Mar 14.
40. Parmenion Capital Partners. The defence dilemma - defence stocks and ESG. Bristol: Parmenion; 2025.
41. PBS NewsHour. Elon Musk's refusal to provide Starlink support for Ukraine attack in Crimea raises questions for Pentagon. Arlington: PBS; 2023 Sep 12.
42. Yale Daily News. Yale professor and student assistants expand viral list of companies leaving Russia initiative. New Haven: Yale Daily News; 2022 Sep 6.
43. TechCrunch. Google pauses its ad sales in Russia, Microsoft pauses sales. San Francisco: TechCrunch; 2022 Mar 4.
44. eMarketer (Insider Intelligence). Big Tech struggles to respond to war in Ukraine. New York: eMarketer; 2022 Mar 1.
45. TechCrunch. Amazon, Microsoft and Google have suspended cloud sales in Russia. San Francisco: TechCrunch; 2022 Mar 10.
46. Courthouse News Service. Tech companies cut ties with Russia over Ukraine invasion. Pasadena: Courthouse News; 2022 Mar 2.
47. Center for European Policy Analysis (CEPA). Should Elon Musk Decide Who Wins Wars? Washington (DC): CEPA; 2024 Feb 29.
48. PBS NewsHour. [See ref 41.]
49. Irregular Warfare Initiative. When a CEO Plays President: Musk, Starlink, and the War in Ukraine. 2025 Jan 10.
50. Axios. Senators call for answers from DOD on Musk's use of Starlink in Ukraine. Washington (DC): Axios; 2023 Sep 13.
51. Al Jazeera. Elon Musk denies selling Starlink to Russia after Ukraine claims use in war. Doha: Al Jazeera; 2024 Feb 13.
52. Euronews. [See ref 6.]
53. PressReader. Outrage over executive's "weaponized" comments. The Denver Post. 2023 Feb 10.
54. Investments (Lloyds Bank/Bank of Scotland). Defence and ESG: A necessary rethink for European investors. 2025.

55. interactive investor. Is there ever a case for defence stocks in sustainable funds? London: ii; 2023 Sep 19.
56. Van Hyfte W. Weapons Manufacturing Is Not Sustainable. No Ifs Or Buts. WealthBriefing. 2024.
57. Don't Bank on the Bomb. Are ESG norms starving the defense industry of capital? The sector's record profits tell a different story. 2024.
58. Duffy A. From Exclusion to Engagement: The Evolving ESG Lens on Defence. ILIM Market Insights; 2025.
59. Euro-SD. Global spending hike in 2024. Bonn: Euro-SD; 2025 May.
60. Harici. Global military spending hits record high in 2024, SIPRI reports. 2025.
61. Tribune India. Global military spending soars to USD 2.7 trillion in 2024; Russia, US, China, India, Germany account for 60%. Chandigarh: Tribune India; 2025.
62. Babel.ua. SIPRI: Global military spending rose to record high in 2024 — here's who's leading. Kyiv: Babel; 2025.
63. Stockholm International Peace Research Institute (SIPRI). Trends in World Military Expenditure, 2024. Stockholm: SIPRI; 2025 Apr 28.
64. Friedman M. [See ref 12.]
65. Digital Trends. Tech's Russia withdrawal might be doing more harm than good. 2022 Mar 24.
66. Inquirer.com. [See ref 38.]