Redefining ‘Responsible Exit’ in the Context of the Crime of Aggression

Lessons from Corporate Responses to Russia’s War Against Ukraine

B4Ukraine

Photo by Romana Yasynovska

EXECUTIVE SUMMARY

The full-scale invasion of Ukraine in 2022 triggered an unprecedented wave of corporate announcements regarding suspension, withdrawal, or continued operations in Russia. Yet four years into the war, there remains no widely accepted framework for what constitutes a responsible corporate exit in the context of a war of aggression. Public debate has often focused on whether companies should stay or leave, while paying less attention to how disengagement should be carried out and how to manage the human rights impacts associated with both staying and leaving. This report addresses that gap by proposing a framework for assessing responsible corporate exit grounded in international business and human rights standards and informed by corporate practice in Russia since 2022.

The framework defines responsible exit as a time-bound, rights-based exit that prioritises immediate harm reduction, avoids causing or contributing to international crimes, applies heightened conflict-sensitive human rights due diligence, prevents the transfer of value or capabilities to abusive actors, and provides remedy and support for affected workers and communities. In the context of a war of aggression, continued economic activity may sustain the aggressor state's fiscal capacity, economic resilience, or technological capabilities, thereby contributing to the continuation of unlawful violence and associated human rights abuses.

This framework also expands the way "relevant stakeholders" are understood in corporate human rights due diligence. Corporate assessments have traditionally focused on individuals within the immediate orbit of company operations, such as employees, suppliers, and local communities. In the context of an aggressive war, however, the harms linked to corporate activity extend beyond these boundaries. Economic activity that contributes to the aggressor state's war capacity can foreseeably sustain harms affecting civilians beyond the company's operational footprint.

A central feature of responsible exit is the need to navigate difficult trade-offs. In practice, there are seldom perfect outcomes. Rapid disengagement may create economic disruption for workers or communities, while prolonged presence risks contributing to an unlawful war. Responsible exit therefore requires companies to balance these competing risks through a structured due diligence process that prioritises the prevention of the most severe harms.

1. INTRODUCTION

This paper is produced by B4Ukraine, a global coalition of civil society organisations working to reduce the economic resources enabling Russia's war of aggression against Ukraine. The coalition advocates for responsible corporate conduct and calls on companies to end business activities in Russia in order to avoid contributing to the financing of the war and to uphold international human rights and humanitarian law. The report was developed in collaboration with the Business and Human Rights Centre (BHRC), a global organisation that tracks the human rights impacts of companies and promotes corporate accountability; the Human Rights Centre at the University of Essex, a leading academic institution working on international human rights law and business and human rights; the Kyiv School of Economics (KSE), whose research has extensively documented the economic role of foreign companies operating in Russia since 2022; and the Investor Alliance for Human Rights (IAHR), a global network of institutional investors working to integrate human rights considerations into investment decisions and promote responsible corporate conduct.

Despite the unprecedented scale of corporate responses to Russia's full-scale invasion of Ukraine in 2022, there remains no widely accepted standard for what constitutes a responsible exit in the context of an international war of aggression. Public debate has often focused on whether companies should stay or leave, while paying less attention to how disengagement should be carried out, how quickly it should occur, and what safeguards are necessary to avoid further harm or unintended consequences. At the same time, the concept of "responsible exit" has sometimes been invoked to justify, delay, or continue operations, even where ongoing business activity contributes financially, materially, or otherwise to Russia's war effort. This paper addresses that gap by proposing a clear framework for assessing responsible corporate exit in the context of the crime of aggression. The context of aggressive warfare involves a particularly clear risk that continued economic activity may contribute to the aggressor state's capacity to sustain unlawful violence and associated human rights abuses. Unlike many conflict situations where responsibility and legal characterisation may be contested, wars of aggression typically involve a clearly identifiable aggressor state and a well-documented pattern of violations, making the link between economic activity, state revenue, and the continuation of the war more foreseeable for the companies.

Drawing on the UN Guiding Principles on Business and Human Rights, international humanitarian law, and corporate practice since 2022, the paper sets out practical criteria for responsible disengagement and particularly what that means four years into the war against Ukraine. These include immediate harm reduction, avoiding corporate complicity in international crimes, applying heightened and conflict-sensitive human rights due diligence, preventing the transfer of value or capabilities to abusive actors, and providing remedy and support for affected workers and communities. The framework is intended to guide companies in planning and implementing responsible exits, support governments and regulators in developing clearer expectations and policy responses, and equip investors and business and human rights stakeholders with metrics to assess corporate conduct in situations where economic activity risks sustaining an unlawful war. Since the full-scale invasion, B4Ukraine has contacted more than 250 companies that continue to

operate in Russia to initiate dialogue about their ongoing business activities and relationships in the country that may contribute to, or be associated with, human rights harms. The insights gathered through these engagements form the foundation of this report.

KEY RECOMMENDATIONS

Companies

- Conduct heightened, conflict-sensitive human rights due diligence when operating in or connected to a state engaged in an unlawful war of aggression to avoid complicity in international crimes, and reassess these risks regularly as the conflict evolves.
- Prioritise immediate harm reduction by promptly suspending or ending activities that generate revenue, taxes, or other economic support for the aggressor state's war effort.
- Develop and implement responsible exit strategies that include clear timelines, stakeholder consultation, and mitigation measures for affected workers and communities affected by the exit, grounded in comprehensive and ongoing Human Rights Due Diligence (HRDD) mechanisms.
- Avoid transferring value, assets, or capabilities to state-linked or abusive actors during exit, including through discounted sales, technology transfer, or continued provision of services, as far as possible.

Governments and Regulators

- Provide clear policy guidance to companies operating in aggressor states, clarifying expectations regarding responsible exit and the risks of corporate complicity in international crimes.
- Align sanctions, trade, and corporate accountability frameworks with business and human rights standards, ensuring companies are incentivised to disengage from economic activities that sustain unlawful wars.
- Support responsible corporate exit through regulatory clarity, licensing mechanisms where necessary, and diplomatic engagement that facilitates disengagement while preventing value transfer to abusive actors.
- Move beyond voluntary measures to strengthen corporate accountability mechanisms, including corporate due diligence and disclosure legislation and enforcement tools, to address corporate contributions to serious human rights abuses and international crimes.

Investors and Business and Human Rights Stakeholders

- Integrate responsible exit expectations into investment decision-making and stewardship activities, including engagement with companies operating in aggressor states, up to and including divestment where necessary.
- Use clear metrics to assess corporate conduct, including assessing financial contributions to the aggressor state, progress toward disengagement, and measures taken to prevent value transfer.
- Encourage transparent disclosure from companies regarding their operations, financial flows, and exit plans in conflict-affected contexts.
- Support collective investor and stakeholder engagement to accelerate responsible corporate disengagement and strengthen expectations around business conduct in situations of armed conflict.

2. CONCEPT AND DEFINITIONS OF ‘RESPONSIBLE EXIT’

UN DEFINITIONS

While there is no single UN definition of responsible exit, the Office of the High Commissioner on Human Rights (OHCHR) standard comes from the UN Guiding Principles on Business and Human Rights (UNGPs, endorsed by the UN Human Rights Council), which implicitly define what a responsible exit means. A responsible exit could be described as an outcome of implementing the corporate responsibility to respect human rights as set out in the UNGPs, where ongoing or proposed operations are assessed through human rights due diligence and a business concludes that remaining would be inconsistent with respect for human rights, and where exit is managed in a way that mitigates adverse impacts associated with the exit itself.

In Remedy in Development Finance, the OHCHR examines responsible exit in the context of development finance institutions (DFIs). DFIs have traditionally focused on environmental and social safeguards at project entry, while exit has often been treated as a financial endpoint rather than a moment of heightened risk. This imbalance is particularly evident in private sector operations, where shorter project cycles accelerate disengagement and reduce transparency. A responsible exit therefore recognises that leaving a project does not end responsibilities for remedy, especially where financiers contributed to harm or where exit creates foreseeable impacts. Exit should be treated as part of core risk management, supported by post-exit monitoring to ensure action plans are completed and grievances addressed. Without such oversight, safeguard systems risk being strongest at entry and weakest when stakeholders are most vulnerable.

Operationalising responsible exit requires embedding it in legal agreements and routine practices. Loan and investment documents should include environmental and social obligations that apply at and after exit, such as criteria for future buyers and provisions securing funds for remedy. DFIs can also extend leverage through coordination with co-investors, engagement with authorities, and post-exit action plans, ensuring projects do not end with unremediated harms.

ACADEMIC INSIGHTS

Recent (limited) academic literature in the business and human rights field has started to delineate what constitutes a “responsible exit” for companies leaving conflict-affected or high-risk areas.

A 2024 study by Thein et al. defines a “responsible exit” through a multi-faceted set of criteria aimed at ensuring that an exit does not simply amount to a “cut and run.” However, while this literature offers useful insights, it primarily examines corporate exits in contexts of political repression and sanctioned regimes rather than in situations of ongoing international armed conflict or wars of aggression. As a result, additional considerations arise in such contexts, including the risk that continued corporate activity contributes to the economic capacity of an aggressor state or creates forms of corporate complicity in international crimes. In the Russian context, for example, assumptions about transparency around exit plans may not

always hold: public disclosure of exit strategies can expose employees to immediate risks, including detention, or undermine other responsible exit measures such as the secure removal of intellectual property or sensitive assets. In Thein et al.'s framework, a responsible exit is an approach that prioritizes:

- Ensuring the company's actions respect legal and normative standards, maintaining legitimacy in the eyes of stakeholders.
- Conducting thorough heightened human rights due diligence (hHRDD) and frequent audits, in line with the UNGPs and the OECD Guidelines for Multinational Enterprises. This means proactively identifying risks associated with both staying and leaving.
- Responsiveness and clear communication with stakeholders (employees, local communities, customers, etc.) throughout the exit process. Transparency about exit plans and considerations is seen as vital to mitigate rumours and uncertainty.
- Strict adherence to international human rights and labour rights principles during the exit. This involves avoiding any actions that would directly or indirectly violate human rights – for example, ensuring that the mode of exit does not lead to rights abuses (such as handing over operations to a perpetrator of abuses).
- Safeguarding employee safety, well-being, and providing fair compensation or support during and after the exit. Responsible exits should strive to minimize the harm to local staff – e.g. by offering severance, facilitating new employment, or even evacuating employees if they face danger.
- Ensuring that assets, operations, or licenses are not simply left in the hands of unscrupulous or sanctioned actors.

In other words, a company should avoid selling or transferring its business to local cronies, human rights abusers, or others who might worsen the conflict or abuse, even if doing so would be the easiest way to leave.

This academic definition underscores that a "responsible exit" is not the same as an immediate exit at any cost, but a managed process aligned with corporate responsibility principles. Through interviews and case analysis in the context of Myanmar's 2021 coup, Thein et al. found that many firms "exiting voluntarily" under stakeholder pressure did so irresponsibly, for example by hastily transferring assets to unethical buyers or failing to protect local stakeholders. Their findings illustrate that exit can be voluntary yet still irresponsible if it harms human rights, underscoring the need for clearer responsible-exit guidelines in high-risk contexts.

POLICY AND NGO DEFINITIONS

In The Business of Leaving, B4Ukraine defines responsible exit as "an approach in line with heightened human rights due diligence under the UN Guiding Principles on Business and Human Rights, which strikes a balance between reducing the negative human rights impacts of exiting while avoiding complicity or complacency in war crimes." In simpler terms, this means a company should weigh the harm its departure might cause (to employees, local populations, consumers, etc.) against the harm of staying (which could include becoming complicit in an oppressive regime's abuses or in an illegal war). The goal is to find an exit strategy that minimizes harm on both sides: mitigating local fallout from withdrawal, while also

ensuring the company is not contributing to or tacitly abetting grave human rights violations by continuing operations.

B4Ukraine's research found that many multinationals remaining in Russia after the 2022 invasion cited "the negative human rights impact of leaving" as a justification for staying; for example, claiming that their products are essential for the local population or that they must protect their Russian employees. However, the research evidences that most such companies did not conduct adequate heightened due diligence to substantiate these claims. In other words, the concept of "responsible exit" is sometimes misused to excuse inaction: companies emphasise the harms of exit but fail to seriously examine how those harms might be mitigated or how staying might entrench other harms. True responsible exit, according to this view, requires a genuine effort to plan and execute the exit in a way that respects human rights, rather than a *carte blanche* to remain indefinitely.

In the British Institute of International and Comparative Law (BIICL) 2022 commentary Pietropaoli and Aguirre stress that "responsible exit must be planned, rights and conflict-sensitive, [and] based on stakeholder consultation through a HRDD process that identifies and attempts to prevent or mitigate negative impacts on human rights." They emphasize that a responsible exit is proactive, not reactive, that it cannot be improvised in the middle of a crisis, but should be part of contingency planning before conflicts escalate. For example, if a company operating in a region had conducted conflict-sensitive due diligence earlier, it might have identified stakeholders at risk (employees, customers, local communities) and planned how to protect them if the security situation deteriorates. BIICL's analysis aligns with the UN Guiding Principles' notion of heightened due diligence in conflict areas, noting that the UNGPs call for expanded stakeholder consultations and conflict analysis in such contexts. In sum, the perspective reinforces that how a company leaves is as important as the decision to leave and that it should not be a panic-driven divestment but a responsibly managed disengagement considering all human rights implications.

The Institute for Human Rights and Business (IHRB) states that companies sometimes face a dilemma: "while in some situations it may be irresponsible not to disengage, equally, cutting and running does not conform with responsible business conduct expectations." The urgency to stop contributing to abuses (e.g. by cutting off a revenue stream to an aggressor state or abusive partner) must be tempered with the duty to avoid new harms caused by a hasty exit. IHRB and others highlight that "moving fast and acting justly are not mutually exclusive." In other words, a company can and should act swiftly to cease involvement in egregious harm, but even swift action can be taken in a thoughtful, consultative way (for instance, communicating with workers, securing data, providing remedies) rather than an abrupt exit.

OECD NCP FINDINGS

Moreover, it may be useful to review the emerging practice under the OECD Guidelines for Multinational Enterprises, particularly through National Contact Point (NCP) decisions. Although these cases arise in contexts different from Russia's war against Ukraine, most notably Myanmar following the 2021 military coup, they provide concrete interpretations of how responsible disengagement should be assessed under established business and human rights standards.

Two recent NCP cases are particularly relevant: Publish What You Pay Australia and Myanmar CSOs v. Myanmar Metals (now Mallee Resources) before the Australian NCP, and SOMO (representing Myanmar CSOs) v. Telenor ASA before the Norwegian NCP. In both cases, civil society organisations challenged whether companies had carried out adequate human rights due diligence when disengaging from Myanmar. The NCPs examined not only the decision to exit but also the process of disengagement, including whether companies had meaningfully engaged stakeholders, assessed the human rights risks of asset transfers, and taken steps to mitigate harms linked to their withdrawal.

The NCP final statements offer useful guidance on responsible exit, particularly regarding stakeholder engagement and due diligence in disengagement decisions. At the same time, experiences in Myanmar highlight the practical limits of transparency and engagement in authoritarian contexts, where public disclosure of exit plans may create additional risks for workers, civil society actors, or the integrity of the exit process itself. These cases therefore provide valuable interpretive guidance while reinforcing the need to adapt responsible exit principles to the specific dynamics of contexts such as Russia's ongoing war of aggression.

INFOBOX I: Legal and Normative Foundations for Responsible Corporate Exit

The concept of responsible corporate exit in the context of Russia's war against Ukraine is grounded in established international business and human rights frameworks.

UN Guiding Principles on Business and Human Rights (UNGPs): The UNGPs establish the corporate responsibility to respect human rights and to avoid causing or contributing to adverse impacts. This corporate responsibility to respect exists independently of states fulfilling their duty to protect human rights. Guiding Principle 7 highlights that companies operating in conflict-affected areas face heightened risks of involvement in gross abuses and should conduct enhanced due diligence. Where such risks cannot be prevented or mitigated, companies are expected to consider disengagement as per UNGP 19.

UN Global Compact: Principle 2 requires businesses to ensure they are not complicit in human rights abuses. The Global Compact emphasizes that complicity may arise not only through direct involvement but also where companies knowingly enable or benefit from abusive systems.

International Human Rights Law (IHRL): Although IHRL obligations formally bind states, they establish the baseline standards that companies are expected to respect under the UNGP framework. States also have a duty to protect against corporate involvement in serious human rights abuses.

International Humanitarian Law (IHL) and International Criminal Law (ICL): IHL prohibits attacks on civilians and other conduct widely documented in Russia's war against Ukraine. Under principles of aiding and abetting liability, individuals, and in some jurisdictions corporations, may face legal accountability where they knowingly provide practical assistance that substantially contributes to international crimes. Likewise, the UNGP Principle 12 Commentary explains that businesses should respect IHL in situations of armed conflict.

Together, these frameworks reinforce the expectation that companies should avoid contributing to or enabling unlawful violence and should disengage where continued operations risk involvement in serious human rights abuses.

3. STEPS, EVENTS, AND MECHANISMS PRECEDING AN EXIT

A corporate exit from a market like Russia, especially one carried out to avoid human rights harm, should ideally be the result of careful planning and be executed responsibly. Several steps, events, and mechanisms typically precede an exit under the heightened due diligence framework.

The first step is a thorough assessment of how the company's operations intersect with the conflict and potential human rights impacts. Companies should undertake heightened human rights due diligence (hHRDD) when entering or operating in high-risk markets or when a conflict escalates.[1] This process requires identifying actual and potential harms connected to the business, including whether products or services may support military activities, whether taxes or other payments contribute to the aggressor state's capacity to wage or sustain war, or whether domestic legislation requires companies to support the war effort. Stakeholder consultation with employees, affected communities, and human rights experts should form part of this process. Where due diligence identifies a risk of involvement in gross abuses that cannot be mitigated, disengagement becomes a necessary option. The UNGPs emphasize that companies should avoid causing or contributing to severe harm and should consider ceasing involvement where such risks cannot be addressed.

A range of external and internal events can precipitate a decision to exit. Sanctions or export controls imposed by home states or international bodies may legally require companies to suspend or terminate certain operations. Host-country legislation can also alter the risk calculus. In Russia, for example, laws requiring businesses to assist with mobilisation or other war-related activities forced companies to confront the possibility of becoming directly involved in the war effort. In addition to legal pressures, investor expectations, shareholder resolutions, civil society campaigns, and reputational exposure can also prompt companies to reassess their continued presence.

Once a decision to disengage is considered, companies must develop a clear exit strategy. Ideally, such plans should exist before a crisis occurs, particularly for operations in high-risk environments. In practice, however, many companies had to design exit strategies rapidly following Russia's full-scale invasion in 2022. Key components of an exit strategy should include:

- **Timeline and Mode:** Companies must determine whether to suspend operations, wind them down gradually, or pursue a full divestment or closure. Exit should be organised and deliberate, but planning must not serve as a justification for prolonged presence.
- **Stakeholder Communication:** Companies should consider how to communicate exit decisions to employees, partners, and customers in order to manage expectations and mitigate disruption. Where feasible and safe, consultation with stakeholders can help reduce negative impacts. In authoritarian contexts, however, transparency may also carry risks and should therefore be assessed carefully.

1. Particular for businesses with operations in Russia, heightened human rights due diligence should have been engaged since the 2014 occupation of Crimea.

- **Mitigation Measures for Affected Parties:** Responsible exit strategies should seek to minimise adverse effects on workers and communities that relied on the business. This may include severance payments, temporary continuation of benefits, relocation support for employees at risk, or coordination with humanitarian organisations where companies previously provided essential goods or services.
- **Asset Disposition:** Companies must decide how to handle physical assets and operations. Options may include sale to an independent buyer, transfer to local management, or abandonment. In Russia, identifying truly independent buyers has often proved difficult, further reinforcing the requirement for careful contingency planning. Exit strategies may also involve legal tools such as sanctions clauses, *force majeure* provisions, or international arbitration if assets are expropriated.

Several external mechanisms can facilitate or accelerate exit decisions. Government advisories urging companies to withdraw can provide boards with political and legal justification. Industry coordination can also reduce competitive disadvantages when multiple firms leave simultaneously. International organisations such as the OECD and UNDP have issued guidance on responsible disengagement from conflict-affected areas. Civil society initiatives, including databases tracking corporate presence in Russia, have also played a role in increasing transparency and applying pressure to companies that remain.

Throughout the process, companies must balance careful planning with the need for timely action. Poorly planned exits can create additional harms, but excessive delay may prolong contribution to human rights abuses and increase the risk of asset seizure or reputational damage. Ideally, companies should initiate exit as soon as due diligence confirms that their activities are linked to harms that cannot be prevented or mitigated.

The experience of corporate withdrawals from Russia since 2022 illustrates this dynamic. Many companies announced suspensions shortly after the invasion and completed their exits within months. Others delayed disengagement due to operational or regulatory obstacles, often facing growing political and reputational pressure. In several cases, prolonged presence ultimately resulted in forced asset transfers or expropriation by Russian authorities. In brief, the sooner the preparatory steps begin, the smoother and earlier the exit can occur.

Conversely, more commonly in 2025, Russia proceeded with expropriating a significant number of company operations still engaged in the market. Rockwool, for example, often justified the company's reluctance to leave saying: "We do not see how handing over more income and a well-functioning business to the Russian state [...] would contribute to ending the war more quickly." In January 2026, Rockwool's four Russian factories were expropriated. Shortly afterwards, Danwatch reported that Rockwool's Russian subsidiary announced that it was donating 600 million rubles to Putin's All-Russia People's Front to support Russian soldiers, with the funds earmarked for drones, vehicles, communications gear and electronic-warfare systems. The same statement declares that Rockwool in Russia will resume cooperation with the military-industrial complex. These developments call into question the company's earlier justification for remaining in Russia and illustrate how delayed exit can ultimately result in assets and resources becoming integrated into the aggressor state's war effort.

In conclusion, a responsible exit is typically preceded by conflict-sensitive due diligence, trigger events that alter the risk environment, and the development of a structured disengagement plan. One clear trigger is a country initiating an aggressive, illegal war. Companies operating in high-risk environments should incorporate exit planning into their overall risk management strategies from the outset. When circumstances change and continued operations become incompatible with human rights and humanitarian law, these plans should be activated without delay. Properly implemented, a responsible exit allows companies to reduce harm while avoiding both chaotic withdrawal and continued involvement in abusive contexts.

INFOBOX II: <u>Cause, Contribute, Directly Linked?</u>

Under the UN Guiding Principles on Business and Human Rights (UNGPs), companies may be involved in human rights harms in three ways: by causing, contributing to, or being directly linked to abuses through their operations, products, services, or business relationships.

A company causes harm when its own activities directly result in human rights violations. It contributes to harm when its actions enable, facilitate, or incentivise abuses carried out by another actor. For example, knowingly supplying dual-use technologies, surveillance tools, or financial services that enable military operations may create a risk that a company contributes to war crimes.

A company is directly linked to harm when abuses occur through its business relationships, even if the company did not cause or contribute to the violations itself. In such cases, the UNGPs expect companies to use their leverage to prevent or mitigate harm and to disengage where mitigation is not possible.

In the context of Russia's war against Ukraine, risks of corporate involvement may arise through continued tax payments to the state (although this is contested), compliance with legislation requiring support for mobilisation or military production, or commercial activities that sustain the war economy. These examples illustrate how ordinary business operations can become connected to an unlawful war. If a company causes or contributes to harm, it is expected to cease, prevent, and remedy that harm.

RESPONSIBLE CORPORATE EXIT FROM RUSSIA

PRE-EXIT STEPS, EVENTS, AND MECHANISMS

1 HEIGHTENED DUE DILIGENCE

Assess how operations intersect with conflict and potential human rights impacts.

- Identify actual and potential harms
- Consider links to military activities, taxes/other payments, and domestic laws supporting war
- Consult stakeholders (employees, communities, experts)
- If risks of involvement in gross abuses cannot be mitigated → disengagement is necessary

UNGPS: Avoid causing or contributing to severe harm; cease involvement if risks cannot be addressed.

2 TRIGGER EVENTS: EXTERNAL & INTERNAL

Events that change the risk calculus and prompt reassessment.

- Sanctions or export controls
- Host-country legislation (e.g., mobilisation or war-support laws)
- Investor expectations and shareholder resolutions
- Civil society campaigns and public scrutiny
- Reputational exposure and political pressure

3 DECISION TO DISENGAGE

Board/management determines that continued operations are incompatible with human rights and humanitarian law.

4 DEVELOP EXIT STRATEGY

Design a clear, structured disengagement plan.

Timeline & Mode

Suspend, wind down gradually, or fully divest/close. Planning should not be used to justify delay.

Stakeholder Communication

Inform employees, partners, customers; consult where feasible and safe; assess risks of transparency.

Mitigation Measures for Affected Parties

Minimise harm to workers & communities. Offer severance, continued benefits, relocation. Coordinate with humanitarian actors if needed.

Asset Disposition

Sell to independent buyer, transfer to local management, or abandon. Use legal tools (sanctions clauses, force majeure, arbitration) if expropriated.

5 IMPLEMENT EXIT & MONITOR IMPACTS

Execute the plan and address impacts.

- Complete withdrawal in an orderly manner
- Support affected employees and communities
- Monitor ongoing human rights impacts and adjust
- Document lessons learned for future risk management

UNDER THE UN GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS (UNGPS), COMPANIES MAY BE INVOLVED IN HARMS IN THREE WAYS:

CAUSE

A company causes harm when its own activities directly result in human rights violations.

Example: Directly operating a facility that commits abuses.

CONTRIBUTE

A company contributes to harm when its actions enable, facilitate, or incentivise abuses carried out by another actor.

Example: Supplying dual-use technologies, surveillance tools, or financial services enabling military operations.

DIRECTLY LINKED

A company is directly linked to harm when abuses occur through its business relationships, even if it did not cause or contribute.

Example: Maintaining a business relationship with a Russian partner whose operations are connected to human rights harms arising from the war, without the company causing or contributing to those harms.

RISKS IN THE CONTEXT OF RUSSIA'S WAR AGAINST UKRAINE

Continued tax payments to the state (contested) may support the war effort

Compliance with laws requiring support for mobilisation or military production

Commercial activities that sustain the war economy

B4Ukraine

4. RESPONSIBLE EXIT REDEFINED

Responsible exit is a time-bound, rights-based disengagement from a conflict-affected or high human rights-risk context that (1) **immediately reduces foreseeable harm to people,** (2) **avoids causing or contributing to international crimes or serious human rights abuses,** (3) is grounded in **heightened, conflict-sensitive HRDD** and **transparent stakeholder engagement**, and (4) **prevents transfer of value or capability** to actors reasonably likely to commit abuses while providing (5) **remedy and support** for affected workers and communities.

Due to various possible circumstances and different contexts, this definition may be applicable to a range of conflict-affected and high-risk areas (subject to further research), however, this report focuses on its application in the context of a war of aggression. Consequently, the responsible exit framework developed below places particular emphasis on the need of companies to exit where continued operations risk sustaining an aggressor state's capacity to wage an unlawful war.

Each of the subsections of the definition are explained below in turn.

1. IMMEDIATE REDUCTION OF FORESEEABLE HARM TO PEOPLE

In the context of Russia's ongoing war of aggression against Ukraine, four years into a full-scale international armed conflict marked by widespread and systematic violations of international humanitarian and human rights law, the baseline assumption can no longer be that continued business operations are neutral or merely commercial. Instead, the continued presence of foreign companies in Russia constitutes an ongoing, foreseeable source of harm, both directly and indirectly, to people affected by the war. Immediate harm reduction therefore means the rapid cessation of those business activities that sustain, enable, legitimize, or normalise the continuation of that harm, the effects of which are experienced by the Ukrainian population as the victims of Russia's aggressive war.

This framing also expands the way 'relevant stakeholders' are understood. Corporate human rights due diligence has often focused primarily on individuals within the immediate orbit of company operations, such as employees, suppliers, and local communities. In the context of an aggressive war, however, the harms linked to corporate activity extend beyond these boundaries. Economic activity that contributes to the aggressor state's fiscal capacity, technological capability, or economic resilience can foreseeably sustain the continuation of widespread violence and repression. As a result, the relevant category of affected stakeholders includes not only those directly impacted by company operations, but also civilians harmed by the continuation of the war and individuals subjected to coercion or repression within the war economy.

The harms are well documented, persistent, and structurally linked to the Russian state's ability to wage war. Russia's military campaign has involved mass civilian casualties, forced displacement, deportations, torture, and the destruction of civilian infrastructure. These are part of a sustained pattern of conduct that has been recognised by multiple international bodies as amounting to war crimes and crimes against humanity. Moreover, an increasing number of scholars argue that Russia's widespread and systematic crimes in Ukraine constitute acts of genocide, as they meet all the criteria set out in Article II of the Genocide Convention.

In this context, any economic activity that contributes to state revenue, economic stability, employment, technological capacity, or social normalization within Russia foreseeably supports the continuation of these harms.

Immediate harm reduction therefore cannot be framed as a gradual or marginal improvement in corporate conduct while remaining in the market. It requires a decisive break with business as usual. For companies with ongoing operations in Russia, the most direct and effective way to reduce harm to people is to stop contributing to the Russian war economy without delay. This includes halting revenue generation, tax payments, royalties, and other financial flows that feed into the state budget, as well as ceasing the provision of goods, services, or technologies that may sustain economic resilience or military capacity. Unlike in early or more ambiguous conflict situations, the link between economic activity and human harm in Russia is now sufficiently clear that delay itself becomes a form of contribution.

These contributions can also be identified and measured. Indicators of corporate linkage to harm include tax payments to the state budget, revenues generated within the war economy, provision of goods or services that sustain military supply chains, and compliance with legislation that compels companies to assist mobilisation or other wartime activities. Tracking these financial and operational contributions over time provides a concrete way of assessing whether companies are reducing or continuing to sustain the war economy. Available data illustrates the scale of these contributions. Analysts from the Kyiv School of Economics estimate that foreign companies remaining in Russia have paid roughly $60 billion in taxes since the full-scale invasion, including approximately $20 billion in 2024 alone, equivalent to roughly half of Russia's annual military budget. These figures illustrate how ordinary commercial activity can materially support the fiscal capacity required to sustain the war.

In addition to taxes and operational revenues, foreign companies have also accumulated substantial profits within the Russian financial system. Due to restrictions on dividend repatriation, large volumes of retained earnings remain deposited in Russian banks, where they contribute to domestic liquidity, credit provision, and government bond purchases. In this way, even companies attempting to "wait out" the conflict may indirectly support the financial stability of the war economy.

Framing immediate harm reduction in this way has important implications for corporate incentives. It shifts the focus away from abstract reputational risk or long-term ethical alignment and toward a concrete, measurable, and time sensitive duty to stop doing harm. The longer a company remains active in Russia, the more it can be shown to have foreseeably contributed to the continuation of an unlawful war. A company that exits in year four cannot plausibly claim the same uncertainty or informational limitations that may have existed in early 2022. As the OHCHR's interpretation of the UNGPs makes clear, once a company becomes aware that it is directly linked to adverse human rights impacts and fails to take adequate action to prevent or end that involvement, it may be considered to be contributing to, or even causing, those harms. Continued presence now reflects a conscious choice to tolerate and absorb the known human rights consequences of operating in an aggressor state.

Immediate harm reduction also requires rejecting narratives that frame exit as the primary source of harm. Many companies still present departure from Russia as a decision that would harm Russian employees, consumers, or communities, and therefore as something that must be carefully delayed or avoided. In the current context, this framing inverts the harm analysis. While exit can cause local economic disruption, these harms are qualitatively and quantitatively different from the large scale, cross border, and lethal harms enabled by the continuation of the war. Responsible exit requires recognizing that the most severe and irreversible harms are borne by civilians in Ukraine and by those forcibly mobilised or repressed within Russia. Immediate harm reduction therefore prioritizes preventing death, injury, displacement, and serious rights violations over preventing job losses or reduced consumer choice.

To incentivise companies to leave, immediate harm reduction should be framed as both an ethical and a legal risk management obligation. From a business and human rights perspective, the foreseeability of harm is now such that continued operations expose companies to heightened potential of complicity, including future legal, regulatory, and civil liability. Companies that can demonstrate prompt exit can credibly argue that they acted to cease contribution once the harm became unavoidable and unmitigable. Companies that remain cannot. Immediate harm reduction thus becomes a form of ex ante risk mitigation.

Finally, immediate harm reduction in Russia must be framed as an achievable and realistic action. Hundreds of companies have already exited or suspended operations, often at significant financial cost, demonstrating that exit is possible even under hostile legal and political conditions. This precedent undermines claims that staying is unavoidable or that exit would cause chaos.

In sum, in the Russian context four years into an aggressive war, immediately reducing foreseeable harm to people means promptly ending business activities that sustain an unlawful war and its attendant human rights abuses. It means recognizing that time itself is a contributor of harm and that exit is the most effective tool available to companies to stop doing damage.

2. AVOIDS CAUSING OR CONTRIBUTING TO INTERNATIONAL CRIMES OR SERIOUS HUMAN RIGHTS ABUSES

The requirement that a responsible exit must “avoid causing or contributing to international crimes or serious human rights abuses” must be understood through the distinctions in the business and human rights framework between causing harm, contributing to harm, and being directly linked to harm through business relationships. These distinctions are important in a situation where the primary perpetrator of abuses is a state, but where private economic actors play a critical enabling role.

Under the UNGPs, a company “causes” an adverse human rights impact when “its acts or omissions, without the involvement of other parties, reduces the realization of a right.” In conflict-affected contexts, however, companies are more commonly understood to contribute to harm “where its conduct together with those of others negatively impacts a right”. The UNDP guidance therefore asks whether there is an adverse impact connected to the company’s activities, whether those activities increase the risk of that impact, and whether the activities “in and of themselves [are] sufficient to result in that impact.”

Where there is an adverse impact connected to a company's activities and those activities increase the risk of that impact, but are not "in and of themselves sufficient to result in that impact," the business is considered to be contributing to the adverse impact and is expected to take measures "to cease, prevent, and remedy its contribution." In the context of Russia's war against Ukraine, this framework is particularly relevant where corporate goods, services, or technologies materially enable actors responsible for violations of international humanitarian or human rights law. In such cases, the appropriate response under the UNGPs is to cease or prevent the company's contribution and mitigate remaining impacts through the use of leverage.

In the Russian context, contribution occupies a broader and more pervasive category. Corporate goods, services, or technologies may materially enable actors responsible for violations of international humanitarian or human rights law, even where the company itself is not the direct perpetrator. Contribution may arise where business activities foreseeably increase the likelihood, scale, or severity of abuses carried out by others. In Russia's war economy, this risk arises when foreign companies continue to generate substantial revenue, pay taxes, maintain supply chains, process financial transactions or otherwise support the economic and administrative capacity of a state engaged in widespread violations.

The Russian state's commission of war crimes and serious human rights abuses is extensively documented and widely acknowledged. As a result, companies operating in Russia cannot credibly claim lack of knowledge. Continued operations therefore amount to a knowing contribution to the state's capacity to sustain the war. Tax payments are taken as an example. While taxation is ordinarily a mere legal obligation, in the context of an unlawful war it becomes a foreseeable means of financing military operations and associated atrocities. The scale of foreign corporate tax contributions to Russia's budget, combined with the fungibility of state revenue, means that continued payment materially supports the machinery of abuse. Moreover, it is widely known that Russian law requires businesses to aid and participate in conscription of their employees as well as provision of resources when requested. Avoiding contribution in this context requires disengagement from the revenue generating activities themselves.

The category of direct linkage further reinforces the need for exit, even in cases where companies argue they neither cause nor contribute to harm. A company is directly linked to adverse human rights impacts when those impacts are caused by an entity with which the company has a business relationship, and where the company's products, services, or operations are connected to that relationship. In Russia, this includes relationships with state owned enterprises, financial institutions, logistics providers, or commercial partners that are embedded in the war economy or implicated in abuses. Even if a company does not materially contribute to specific violations, its continued commercial relationships can enable abusive actors to function, profit, or maintain legitimacy.

Under the UNGPs, direct linkage still generates a responsibility to use and increase leverage to prevent or mitigate harm. Where leverage is insufficient or ineffective, disengagement is the appropriate response. In Russia, the ability of foreign companies to exercise meaningful leverage over state actors or state aligned entities is extremely limited, particularly under conditions of authoritarian governance, retaliatory legislation, and expropriation risk.

Continued engagement therefore fails the leverage test. Remaining in the market while abuses persist does not reflect responsible use of influence, but rather acceptance of ongoing linkage to harm. Exit becomes the only credible means of severing that linkage.

Avoiding causation, contribution, and direct linkage also requires rejecting the idea that neutrality is possible in an aggressive war. Economic activity is not neutral when it takes place within a system that mobilizes all available resources toward military objectives and internal repression. Employment provided by foreign firms can feed into forced mobilization; technologies and know-how can be repurposed; corporate presence can be used domestically and internationally to signal economic normalcy and to undermine the effectiveness of sanctions and diplomatic isolation.

Framing this element of responsible exit in these terms strengthens incentives for companies to leave by clarifying that the risk is not limited to egregious or exceptional conduct. Ordinary commercial operations can amount to contribution or linkage when they take place in a context of systematic international crimes. The longer a company remains, the harder it becomes to argue that it has taken all reasonable steps to avoid involvement in serious abuses. Exit, therefore, is the clearest and most defensible way for companies to demonstrate that they have acted to avoid causing, contributing to, or remaining linked to international crimes and human rights violations.

A responsible exit recognizes that when a state is engaged in sustained and unlawful violence, continued economic engagement inevitably implicates private actors in that violence. Disengagement, even at significant cost, is the minimum action required to comply with the responsibility to respect human rights in the face of international crimes.

3. GROUNDED IN HEIGHTENED, CONFLICT-SENSITIVE HRDD

For a responsible exit to be credible in the context of Russia's war of aggression, the application of heightened human rights due diligence (hHRDD) must be a decision-shaping process, and not a tick-box exercise. Four years into the conflict, such due diligence cannot function as a tool for incremental risk management while maintaining operations. Instead, it must operate as a mechanism for confronting the full human rights implications of continued presence and for determining whether disengagement is required to comply with the responsibility to respect human rights.

Applied to Russia, heightened and conflict-sensitive due diligence necessarily begins from the recognition that the operating environment is dominated by an ongoing international aggressive armed conflict involving systematic violations of international humanitarian and human rights law. This context fundamentally alters the risk profile of all business activities. A due diligence process that genuinely reflects this reality must treat the aggressive war as the primary lens for human rights risk.

When applied consistently in the Russian context, such hHRDD leads to a series of conclusions that strongly incentivise exit. First, it establishes that adverse human rights impacts associated with operating in Russia are structural and systemic, and therefore cannot be mitigated through internal procedures. They arise from the nature of the state itself as a primary perpetrator of abuses and from the extensive

and crucial integration of the economy into the war effort. As a result, the scope for preventing or mitigating harm while remaining operational is severely constrained. HHRDD therefore shifts the analysis from how to operate responsibly to whether responsible operation is possible at all.

Second, conflict-sensitive due diligence requires companies to assess not only the harms they directly cause, but also the broader conflict dynamics their presence affects. In Russia, continued foreign business activity contributes to economic resilience, employment stability, technological capacity, and perception of international normalcy. These factors, taken together, reduce the pressure on the state to alter its conduct and can prolong the conflict. A due diligence process that accounts for these dynamics cannot plausibly conclude that continued operations are neutral. Instead, it reveals that remaining in the market carries a foreseeable risk of exacerbating the conflict and the associated human rights abuses, even where the company's products or services are civilian in nature.

Third, applying hHRDD in Russia requires continuous reassessment over time. The fact that some companies may have initially stayed under conditions of uncertainty does not justify continued presence four years later. As the war has persisted, the evidence of atrocities accumulated, and as the Russian legal framework has increasingly compelled corporate alignment with state objectives, the risk landscape has significantly changed. A company that remains must be able to demonstrate that it has revisited its assessments, updated its conclusions, and adapted its actions accordingly. In practice, updated due diligence conducted in 2023, 2024, or 2025 would be expected to reach a different conclusion than one conducted in early 2022. Failure to act on that updated assessment undermines the credibility of the company's due diligence process.

Companies must act consistently with the conclusions of their own risk analysis when that analysis is conducted to the standard required in conflict settings, consistently, and correctly, as described above. The analyses, conducted as such, also increases accountability. If a company claims to have conducted hHRDD yet continues to operate, it must explain how it has concluded that its presence does not exacerbate conflict, does not contribute to state capacity for abuse, and does not expose it to unacceptable risks of human rights violations.

In the context of Russia's war of aggression, heightened human rights due diligence, properly applied, leads toward exit rather than away from it. Exit should therefore be understood as the rule rather than the exception. Remaining in the market becomes the exception and must be justified on the basis of due diligence demonstrating that the company's continued presence does not exacerbate the conflict or contribute to the state's capacity to sustain the war or associated human rights abuses.

4. PREVENTING THE TRANSFER OF VALUE OR CAPABILITY TO ACTORS LIKELY TO COMMIT ABUSES

In Russia, the primary actor reasonably likely to commit abuses is the state itself, along with state owned enterprises, sanctioned entities, and private actors closely aligned with or dependent upon state power. A responsible exit must be structured to ensure that a company's withdrawal does not transfer additional economic value, operational capacity, intellectual property, know-how, or strategic advantage to Russian state actors, the military-industrial complex, or third-party buyers whose

ownership, affiliations, or market role would foreseeably channel similar benefits back to the Russian state.

Transfer of value can occur in multiple ways. The most obvious is the sale of assets, subsidiaries, or operations to state linked or state favoured entities, particularly at discounted prices or under coercive conditions. Such transactions can provide the Russian state or its proxies with functioning businesses, infrastructure, and revenue streams that continue to support the war economy. Even where a company formally exits, selling its operations to an actor embedded in the state apparatus can amount to a de facto continuation of the same economic activity under new ownership, with the added benefit to the state of acquiring assets.

Transfer of capability includes technology, intellectual property, know-how, data, trained personnel, supply chain access, and brand legitimacy. In Russia, these capabilities can be repurposed for military, surveillance, or similar purposes. For example, industrial technologies can be adapted for military production, digital services can enhance state surveillance or information control, and management systems can strengthen state owned enterprises. A responsible exit must not leave behind capabilities that predictably enhance the state's capacity to commit abuses.

Companies often attempt to justify continued operations by arguing that a forced or rushed exit would result in asset seizure or sale to the state or another actor, and that remaining allows them to retain control and prevent misuse. However, continued operation itself transfers value on a daily basis through taxes, employment, production, and normalization. Moreover, delayed exits often end in the same outcome companies claim to be avoiding, namely expropriation or coerced transfer under worse conditions (examples include Rockwool or CANPACK]. Preventing value transfer therefore argues for earlier, not later, disengagement, when companies still have some agency over how assets and capabilities are handled.

Responsible exit in this context may require companies to accept write downs, abandon assets, actions which carry financial costs. In some cases, preventing value transfer may also involve dismantling operations, removing critical equipment, disabling software, withdrawing licenses and patents, or otherwise ensuring that capabilities cannot be easily repurposed. Such measures must be assessed carefully to avoid creating additional harm, but they may be necessary where the alternative is foreseeable misuse by abusive actors.

A workable framework would design responsible exit as capability extraction, meaning the company leaves in a way that (1) removes what can be removed, and (2) disables what cannot be removed, so that the Russian state or state-linked actors cannot inherit a ready-to-run business, usable technology, or valuable know how. In practice, this can include pulling proprietary tooling, withdrawing licenses, shutting off cloud and remote management, terminating maintenance and updates, and carving intellectual property out of any sale so that even if the acquirer gets local assets, it does not inherit the "brains" of the operation. This was done by many major software and services firms ending support or access in Russia, which reduces capability over time by cutting off updates, security patches, and vendor assistance. For example, SAP let maintenance contracts expire and ended support, and Microsoft has suspended services and sales in ways that materially constrain Russian customers' access to ongoing capability.

Furthermore, there are examples of companies choosing non-transfer through destruction of inventory rather than letting it be absorbed into the market. Reportedly, CISCO's Russian subsidiary physically destroyed unsold equipment worth the equivalent of tens of millions of dollars during the wind-down. This shows that exiting can be done in ways that target high-risk assets and prevent them being repurposed.

There are also common exit structures that aim to stop capability transfer even where a business is sold. McDonald's, for example, exited by selling its Russian business and removing its brand from the market, with the successor operating under a new name, which is a form of IP and legitimacy withdrawal even if physical assets stay behind. In brief, the capability removal could include exporting movable high value equipment where legally possible, removing proprietary components and software keys, wiping or retrieving sensitive data and servers, terminating licenses and support, and refusing any sale that transfers trademarks, patents, core process documentation, or specialised tooling particularly to state-linked buyers.

Preventing transfer of value or capability also extends beyond the moment of exit. Companies retain responsibility to ensure that their brands, technologies, and intellectual property are not used post exit for abusive conduct. In Russia, this includes monitoring for unauthorised use, taking legal action where feasible, and publicly disassociating from continued operations conducted under similar names or branding (for example, Michelin). While enforcement may be limited, the effort itself signals that the company does not condone or participate in the continuation of its products and brand being used for harmful purposes.

A responsible exit therefore requires not only leaving, but leaving in a way that does not equip the perpetrator of international crimes with new resources, tools, or legitimacy.

5. REMEDY AND SUPPORT FOR AFFECTED WORKERS AND COMMUNITY

A responsible exit from Russia must include meaningful remedy and support for workers and communities affected by the company's exit, but this obligation must be understood in proportion to the gravity of the surrounding context. Remedy in this setting does not require preserving business operations at all costs, nor does it justify continued presence in a state committing international crimes. Instead, it requires that companies take reasonable, timely measures to mitigate the adverse impacts of exit on individuals who depend on the business, without perpetuating greater harm through ongoing contribution to the war.

The terms remedy and support serve different functions in the business and human rights framework. Remedy refers to measures taken to "counteract, or make good, the adverse impact" where a company has caused or contributed to a human rights harm. By contrast, support measures adopted during disengagement, such as severance, relocation assistance, or employment support, are typically preventive or mitigative in nature. They are intended to reduce foreseeable harms resulting from the company's withdrawal, rather than to repair harms for which the company bears responsibility.

Meaningful remedy and support also require engagement with affected stakeholders. Companies should consult workers, worker representatives, and, where feasible, affected communities in order to understand the potential impacts

of exit and to design mitigation measures that respond to their needs and safety concerns.

For workers, the support and remedy framework means providing fair and dignified exit measures such as severance pay, continuation of benefits for a defined period, assistance with job placement where feasible, and in some cases support for relocation or remote employment. In the Russian context, particular attention must be paid to employee safety, including risks related to forced mobilization, political repression, or retaliation for association with a foreign employer. Responsible support therefore includes avoiding actions that would expose workers to heightened danger as a result of the company's exit, while recognising that continued operation itself may also increase such risks over time.

Evidence from company exits since 2022 shows that providing remedy and support to workers does not require maintaining operations in Russia. Several multinational firms paired their withdrawal with concrete measures to protect employees, including relocation, continued employment abroad, and support for family members. Goldman Sachs facilitated the transfer of Moscow based staff to other jurisdictions, while Deutsche Bank moved IT employees from Moscow and St. Petersburg to Germany. Accenture and Alphabet similarly supported Russian employees and their families who wished to emigrate. These practices are significant because they demonstrate that exit can reduce, rather than increase, risks to workers in a context where remaining employees may face forced mobilization, political repression, or other forms of state coercion. They also directly counter the argument that companies must stay in the market in order to protect their workforce.

For communities and consumers, remedy should focus on preventing sudden deprivation of genuinely essential goods or services, where applicable, and on coordinating with alternative providers or humanitarian actors where feasible. However, claims of community harm must be assessed critically and cannot be used to justify indefinite delay. The loss of employment or commercial presence, while significant, does not outweigh the obligation to avoid contributing to widespread and severe human rights abuses.

Crucially, remedy and support must be framed as complementary to exit, not as a substitute for it. A company cannot discharge its responsibility to respect human rights by treating employees well while continuing to finance or enable an aggressive war. In the Russia context, responsible exit requires holding both imperatives together: ending contribution to harm as quickly as possible, while taking concrete steps to support those directly affected by the company's departure.

5. CASE STUDIES

SOCIÉTÉ GÉNÉRALE: THE ADVANTAGES OF AN EARLY EXIT

- Société Générale publicly announced on 11 April 2022 that it would cease banking and insurance activities in Russia and signed an agreement to sell its stake in Rosbank and related Russian insurance subsidiaries to Interros Capital (described as Rosbank's previous shareholder), aiming for an "effective and orderly manner" exit while "ensuring continuity" for employees and clients. The bank closed the transaction on 18 May 2022, stating it had exited Russia and reporting an expected net loss of around €3.2bn.

- On timing alone, Société Générale's exit is a useful "early exit" benchmark for Russia: it moved from a signed deal (11 April 2022) to completion (18 May 2022), and it publicly framed the move as a clean severing of banking and insurance activities rather than an indefinite "pause." Most importantly, the exit was completed less than three months following Russia's full-scale invasion of Ukraine.

- On the core "harm reduction" dimension, exiting quickly reduced future tax contributions and financial intermediation capacity supporting Russia's economy (a concern particularly acute for banks). On stakeholder protection, Société Générale explicitly framed the exit as orderly and continuity-preserving for employees and clients.

  The main responsible-exit trade-off is value and capability transfer: reporting at the time noted the buyer's link to Vladimir Potanin and characterised the deal as transferring the Russian unit back into his business orbit, prompting criticism that the transaction could be viewed as a windfall to an oligarch. This is important as responsible exit frameworks caution against transferring assets to actors likely to contribute to abuses or benefit materially from aggression.

- Overall, while imperfect, Société Générale remains a strong early example: fast decision-to-execution, clear deconsolidation mechanics, and willingness to take a large financial hit to effect a definitive withdrawal.

UNILEVER: THE DOWNSIDES OF A DELAYED EXIT

- Unilever's Russia footprint included physical manufacturing facilities and a large local workforce. In February 2023 reporting, Unilever noted over 3,000 employees in Russia and (on 31 December 2022), the company had about €900m in Russian assets, including four factories. On 8 March 2022, Unilever condemned the war, stated that it had suspended imports and exports into and out of Russia, would stop media and advertising spend, would not invest further capital, and would not profit from its presence, while continuing to supply "everyday essential food and hygiene products made in Russia." In February 2023, Unilever stated that it had three options:

  1. closing down (which it argued would lead to appropriation and Russian-state operation of its brands/business, and would "abandon" its people),
  2. selling (which it said it had not yet been able to do in a way that safeguarded people and avoided state benefit), or
  3. continuing to run under strict constraints (described as the "best option" at that time).

- Unilever's prolonged presence drew increasing reputational and human rights pressure. In July 2023, the National Agency on Corruption Prevention (NAZK/NACP) added Unilever to its "international sponsors of war" list, citing continued operations in Russia. At the time, Unilever confirmed to B4Ukraine that it would comply with Russian conscription law if staff were called up. Once a host state legally compels support to war mobilisation, the "stay to protect employees" claim clearly inverts: continued operation may itself expose employees to coercive harm and deepen the firm's linkage to the war effort.

- Russian legal and political barriers increased the costs of exits for "unfriendly" countries. By 2024, the Russian government required steep discounts on exit transactions and approvals from Russian authorities, signifying increasingly hostile legislation. For Unilever specifically, September 2024 reporting described Russian government approval for a sale, noting the Kremlin's typical demand for at least a 50% discount on exit deals and referencing valuations of Unilever's Russian assets. On 10 October 2024, Unilever announced it had completed the sale of its Russian subsidiary to Arnest Group, stating the deal included all business in Russia and four factories and also included its Belarus business. Unilever described extensive preparatory work over the preceding year, including separating IT platforms and supply chains, and stated that completion ended Unilever Russia's presence in the country.

- Unilever's trajectory shows both the real operational friction of exiting with physical assets and staff, but also highlights the downside of delay.

  On the positive side, Unilever ultimately did follow through on its exit from Russia, completing the sale of its local business and ending its presence in October 2024. The eventual divestment shows that even after a prolonged period, companies can complete a full exit once disentanglement and internal assessments are carried out and insisted upon.

  At the same time, the case illustrates the shortcomings of a reactive rather than proactive approach to exit. Unilever continued local production in Russia for more than two years after the full-scale invasion, maintaining tax payments and economic activity that could reasonably be interpreted as contributing to, or at minimum being directly linked to, harms associated with Russia's war of aggression. This prolonged presence exposed the company to sustained criticism, including Ukraine's designation of Unilever as an international "war sponsor," and raised questions about whether the company had adequately anticipated and prepared for the possibility of disengagement in a high-risk context. The extended delay also weakened claims that continued operations were primarily intended to protect employees, given the mobilisation and coercion risks associated with remaining in the Russian war economy. This suggests that earlier engagement in a conflict-sensitive hHRDD and more decisive action could have significantly reduced the period during which Unilever remained exposed to risks in the Russian market.

  Overall, the Unilever case occupies a middle ground. It demonstrates that full disengagement from Russia remains possible even after a prolonged delay, but also illustrates why companies operating in high-risk environments must be better prepared to exit more rapidly when the risk of contributing to serious human rights abuses becomes clear.

RAIFFEISEN BANK INTERNATIONAL (RBI): THE CONSEQUENCES OF STAYING

Raiffeisen Bank International represents the clearest example of irresponsible non-exit among Western companies operating in Russia since the full-scale invasion of Ukraine. The bank remains widely described as the largest Western financial institution still active in the Russian market and continues to play a significant role in facilitating cross-border trade and payments. Its Russian subsidiary serves millions of retail and corporate clients and has remained one of the limited channels through which companies in Russia can access international payment systems, including connections to the SWIFT network. Reporting characterises these functions as forming part of the financial architecture that allows the Russian economy to continue operating under wartime sanctions conditions. The bank's Russian branch continues to play a "systemically important" role in the Russian economy, according to the Russian Central Bank, generating over €6 billion since the full-scale invasion began In the context of an aggressive war, such financial intermediation cannot plausibly be treated as neutral. Banking services sustain trade flows, enable tax generation, support corporate activity, and help normalise economic life. Instead of prioritising the immediate reduction of harm as characterised in this report, RBI has continued to operate a large-scale financial platform inside the Russian economy years into the conflict.

The bank's public messaging since the invasion illustrates a pattern of delay rather than a credible attempt at an exit strategy. Early statements in 2022 alternated between suggesting the bank was considering leaving Russia and asserting that it had no plans to withdraw. Instead of establishing a clear disengagement timeline aligned with heightened human rights due diligence expectations in conflict areas, RBI repeatedly attempted to justify delay by pointing to operational constraints, regulatory complexity, and the need to protect shareholder value. This approach conflicts directly with the responsible exit principle that companies operating in high-risk areas must prioritise rapid harm reduction once the risk of contributing to human rights abuses becomes clear.

The scale of RBI's continued financial activity in Russia underscores the severity of this failure. RBI's has made substantial tax payments to the Russian state and the profitability of its Russian subsidiary has been significant since the start of the war. RBI paid approximately $491 million in taxes in Russia in 2023 alone, making it by far the largest foreign corporate taxpayer in the country within the relevant dataset. Separate analysis indicates that the bank has paid more than €1.3 billion in taxes since the invasion began. These figures show the mechanisms through which continued operations translate into Russia's capacity to wage its illegal war. In wartime conditions, taxes, payment services, and financial intermediation are predictable channels through which the Russian state maintains fiscal resources and economic resilience. From the perspective of responsible exit, these payments represent precisely the kind of contribution to harm that companies should seek to terminate as quickly as possible.

RBI has repeatedly tried to justify its failure to exit by pointing to legal barriers, regulatory approvals, and the complexity of disentangling a major banking operation from the Russian economy. Senior executives have described scenarios in which the bank might sell only part of its Russian operations while retaining a minority stake, while also emphasising the difficulty of extracting profits that have accumulated inside Russia since the invasion. Attempts to recover these funds have

reportedly involved exploring sales to local buyers in exchange for permission to repatriate profits. This approach is inconsistent with responsible exit principles. To put it simply, RBI has subordinated its obligations not to contribute to harm to its financial considerations.

The longer RBI has remained in Russia, the more exposed it is to coercive leverage from the Russian state itself. The bank has faced escalating legal disputes and court actions that threaten significant asset seizures or forced transfers. Russian courts have issued rulings connected to commercial disputes that could allow billions of dollars to be claimed from the bank's Russian operations. These developments show that delaying withdrawal and favouring profitability can instead increase vulnerability to retaliatory regulation, legal coercion, or forced value extraction. In other words, postponing exit may ultimately cause financial losses anyway, while adding legal, reputational, and human rights risks.

The bank's Russian subsidiary has continued to provide financial services to companies linked to defence supply chains, including firms producing materials used by arms manufacturers. Even if RBI applied hHRDD mechanisms and sanctions screening, the structure of Russia's heavily militarised economy makes it extremely difficult to ensure that commercial relationships are not connected to military production.

Therefore, reports produced by BankTrack and B4Ukraine explicitly recommend that the bank write off its Russian business rather than seek Kremlin approval for a transaction that could transfer assets or strategic value to state-linked actors. When a credible buyer cannot be found without benefiting abusive actors, the responsible course may require accepting economic loss in order to stop contributing to harm.

Viewed through the responsible exit framework used in this report, RBI represents the clearest example of a company failing to meet even the minimum expectations of responsible disengagement. Four years after the invasion, the bank continues to operate a major financial platform inside Russia, generating tax revenue, sustaining payment infrastructure, and enabling economic activity within a wartime economy. Rather than prioritising rapid harm reduction, RBI has pursued a strategy that preserves financial interests while prolonging its role in sustaining the economic systems that support Russia's war effort.

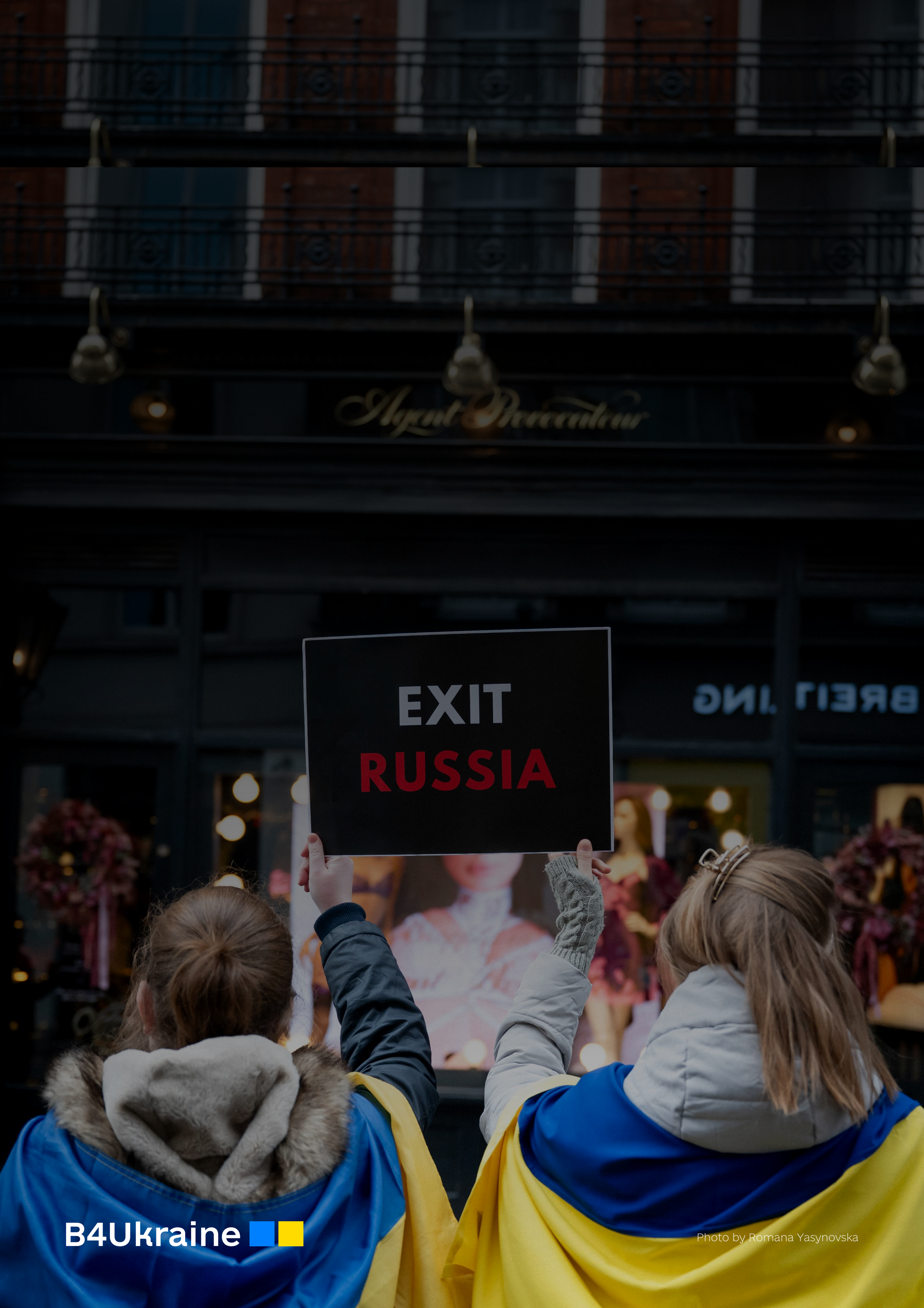

Photo by Romana Yasynovska