Adaptive Policies Designed in Order to Better Support Local Entrepreneurs in the Context of Geopolitical Unrest and War

Diana MARDAROVICI*
Bucharest University of Economic Studies, Bucharest, Romania
**Corresponding author, diana.mardarovici@gmail.com*

Marta Christina SUCIU
Bucharest University of Economic Studies, Romanian Academy,
National Economic Research Institute Costin C. Kiritescu, Interdisciplinary Research Group,
Romanian Academy of Scientists, Bucharest, Romania, International Union
for Interdisciplinarity and Transdisciplinarity in Complex Systems (IUITCS) Belgium
christina.suciu@economie.ase.ro

Abstract. *Geopolitical instability and war make life harder for small and medium-sized businesses, especially in Eastern Europe. The war in Ukraine has thrown trade, supply chains, and financial systems into disarray, leaving local entrepreneurs facing a lot of uncertainty. These shocks call for practical policy changes that help businesses stay afloat. Research so far points to three helpful tools: financial support, more flexible rules, and investments in digital systems. But there's still not enough clear comparison between what works where, especially between different countries in Eastern and Northern Europe. New risks, like cyberattacks and weak digital infrastructure, also deserve more attention. This study looks at how governments in Finland and parts of Central and Eastern Europe have responded. It focuses on three questions: (1) Which policies have actually helped businesses in conflict zones? (2) What impact have financial aid, regulatory tweaks, and digital upgrades had on business resilience? (3) What lessons can we draw for future policy? The study is based on academic research, government documents, and real-world examples. It shows that regional trade deals, producing goods closer to home, and strong digital institutions help companies survive in uncertain times. Cybersecurity and cross-border cooperation also matter more than ever, especially with rising threats from state-led attacks. Our paper aims to bring practical evidence into the conversation on how to support businesses facing geopolitical risks and give policymakers some concrete ideas to work with.*

Keywords: entrepreneurship, policy, governance, economic resilience, SMEs, geopolitical risks, financial support.

Introduction

Geopolitical instability and armed conflict pose significant challenges for economic, social, and political development across macroeconomic, mesoeconomic, and microeconomic levels. This paper concentrates on small and medium-sized enterprises (SMEs), which we view as particularly exposed to external shocks, international tensions, and the increasingly complex and turbulent conditions shaping the global economy. The escalation of conflict following the Russian Federation's invasion of Ukraine has intensified pre-existing structural vulnerabilities, particularly in Eastern Europe, where SMEs are experiencing heightened financial volatility, disrupted logistics, and pressure on institutional capacities (Audretsch et al., 2023; European Bank for Reconstruction and Development [EBRD], 2023).

In regions affected by conflict, SMEs are often hit hardest. Many face cash flow problems, lose access to key markets, and struggle to keep daily operations running. These aren't abstract

DOI: 10.2478/picbe-2025-0351
© 2025 D. Mardarovici; M. C. Suciu, published by Sciendo.
This work is licensed under the Creative Commons Attribution 4.0 License.

issues—they require direct, localised policy solutions that understand the specific conditions on the ground. Keeping a competitive edge in such unstable environments is not about vague resilience; it depends on whether firms can quickly tap into flexible funding sources and benefit from regulations that adapt to their reality (Gamage et al., 2020; OECD, 2023) These conditions demand policy responses that are not only reactive but also capable of enabling long-term sustainability and adaptation.

The existing literature has broadly acknowledged the impact of geopolitical disruptions on entrepreneurship and economic resilience, consistently calling for adaptive policy frameworks that promote business continuity in uncertain environments (Caldara & Iacoviello, 2022; Khan et al., 2023). Prior studies have emphasized the importance of direct financial support, regulatory predictability, investment in digital infrastructure, and cross-border trade cooperation as pillars of SME resilience (Shou et al., 2024; World Bank, 2022). However, a gap remains in comparative empirical analyses that evaluate how specific policy tools perform across diverse geopolitical settings—particularly in Eastern and Northern Europe, where systemic risks intersect with institutional transition challenges (Quak, 2019; Alatalo, 2024).

Moreover, the increasing prevalence of cyberwarfare, including state-sponsored digital threats, has introduced new dimensions of risk that further complicate the operational landscape for SMEs. Emerging forms of cyber aggression, driven in part by advancements in artificial intelligence and the exploitation of digital infrastructure weaknesses, have been flagged in global policy circles as requiring urgent and coordinated responses (Nasheri, 2023; Vasylieva et al., 2024).

In response to these challenges, the present paper adopts a qualitative approach, focusing on policy responses in Finland and selected Central and Eastern European countries. The analysis identifies promising governance mechanisms, financial support instruments, and digital transition strategies that have shown efficacy in preserving SME viability during periods of heightened geopolitical risk. By synthesizing these findings, this paper aims to offer evidence-based recommendations to policymakers engaged in designing economic frameworks resilient to external shocks. In addition, the paper expands the scope of inquiry to include emerging threats to economic security—such as AI-driven cyberattacks and digital vulnerabilities—highlighting the need to incorporate these concerns into national and transnational policy agendas (UNDP, 2023).

Literature review

Key definitions

To build a solid analytical base, this section clarifies several core terms used throughout our paper.

Geopolitical risk refers to the threat that political events—such as war, sanctions, or shifts in international policy—pose to economic stability and business activity. As Caldara and Iacoviello (2022) explain, this includes not only military conflict and trade barriers, but also the realignment of global alliances. In today's context, the term has expanded to include digital threats, such as cyberwarfare, tech-based restrictions, and critical weaknesses in supply chains that now extend far beyond traditional front lines.

Economic resilience describes an economy's capacity to absorb shocks and recover from them. In the face of events like wars or financial disruptions, the presence of stable institutions, responsive fiscal tools, and proactive government measures becomes essential. Khan, Khurshid, and Cifuentes-Faura (2023) argue that digital infrastructure and access to diversified trade routes are now just as crucial as traditional financial safeguards when trying to preserve resilience under pressure.

Small and Medium-Sized Enterprises (SMEs) are generally businesses with fewer than 250 employees and under €50 million in annual revenue. They account for a large share of employment and innovation, but often lack the resources to scale, access international markets, or recover quickly from crisis. Their size can make them agile—but also particularly vulnerable.

Cybersecurity threats have become more sophisticated and more damaging. Hacking, phishing schemes, and state-sponsored attacks increasingly target businesses, including SMEs, often with the goal of stealing data or disrupting operations. According to Nasheri (2023), these attacks have intensified in recent years, and many smaller firms lack the technical capacity or financial means to build strong defenses.

Adaptive policies allow governments to respond flexibly to rapid change—whether economic, political, or technological. These policies include fast-deployed financial support, trade rule adjustments, or digitalisation initiatives that help businesses adapt. Alatalo (2024) notes that successful adaptive policies are not just reactive; they rely on real-time risk analysis and cooperation between public institutions and the private sector.

Theoretical framework

Several theoretical approaches help explain how entrepreneurs keep going when war or instability turns their markets upside down. One that stands out is *Economic Resilience Theory*, put forward by Briguglio et al. in 2009. It argues that resilience is not just about surviving shocks, recovering, and adapting quickly. The key lies in having a mixed economy and policies that can shift when needed. Countries that rely on a single sector, like tourism or oil, suffer more in crises. Those that build strength across sectors—tech, agriculture, logistics—cope better.

Policy also matters. When governments adjust quickly—by easing trade rules, offering emergency credit, or cutting red tape—businesses can breathe. This isn't theoretical. During COVID-19 and the war in Ukraine, countries that acted fast with targeted support saw fewer SME collapses and a faster return to stability.

Institutional theory, as developed by North (1990), adds depth. It shows how both formal systems (laws, courts, regulations) and informal norms (trust, customs, local practices) shape the space in which entrepreneurs operate. In conflict zones, formal systems often break down. What holds things together, at least partially, is trust—who one knows, not what is on paper. In these settings, verbal commitments and informal credit networks matter more than contracts.

That does not mean formal systems do not matter. Where courts function, businesses can plan and invest. Where they do not, risk goes up. In most fragile regions, entrepreneurs rely on a mix—formal rules where possible, informal safety nets when necessary.

The Resource-Based View (RBV), developed by Barney in 1991, shifts the focus to what firms have at their disposal. Resilience here means using one's own strengths—cash reserves, skilled staff, digital tools—to stay afloat. In practice, businesses with cloud systems and online sales platforms adapted far better during the pandemic than those still relying on in-person service. It is the same in war zones: if you have got tools that don't rely on stable infrastructure, you are ahead.

What is "valuable" in this context? Strong IT systems, loyal clients, flexible suppliers, and, increasingly, cybersecurity. These aren't extras anymore—they're survival tools. SMEs with basic digital infrastructure and access to financing can reroute operations, access new markets, or at least maintain cash flow. Without them, even the best business idea collapses.

Khan, Khurshid, and Cifuentes-Faura (2023) show how political instability in Central and Eastern Europe scares off investors and hurts trade. But targeted financial tools help. The EIF's €1

DOI: 10.2478/picbe-2025-0351, pp. 4601-4609, ISSN 2558-9652 |
Proceedings of the 19th International Conference on Business Excellence 2025

billion loan guarantee for SMEs affected by the war in Ukraine made a clear difference. So did Poland's subsidized credit lines for small businesses grappling with broken supply chains.

Alatalo (2024) looks at how Finnish firms handled a combination of political tensions and market volatility. His findings? Stability doesn't just come from institutions—it comes from agility. Trade policy, digital systems, and simple customs procedures helped businesses adjust quickly. The Baltic states show this well: when cross-border rules are simple and predictable, small firms can keep going even when bigger markets are shaken.

Digital readiness is crucial. Estonia's e-Residency or Ukraine's Diia app didn't just modernize bureaucracy—they kept businesses functioning during war. That's not just innovation, it's resilience. These tools let entrepreneurs pay taxes, manage contracts, and communicate—even under siege.

Supply chain resilience also matters. Lithuania's push to localize essential production is about risk control. Poland's deals with neighbors to reroute logistics during the Ukraine conflict show how regional cooperation becomes a resilience strategy.

And then there's cyber risk. Nasheri (2023) clarifies that cyberattacks are now part of geopolitical warfare. State-backed hacks are common, and SMEs are easy targets. Most don't have proper defenses, leaving them open to data theft, disruption, and blackmail. The solution isn't just tech—it's policy. Nasheri calls for stronger cross-border cybersecurity rules, better SME training, and real investment in digital defense.

When you pull these threads together, one thing becomes clear: resilience isn't a buzzword. It's a practical mix of internal capacity, institutional support, and policy agility. SMEs that survive conflict don't just get lucky—they have tools, networks, and backup systems that help them adapt.

Methodology

This study uses a qualitative approach based on case study analysis. The aim is to understand how specific policy responses have supported SMEs in the context of geopolitical instability. The cases examined include Finland and several countries from Central and Eastern Europe. These were selected based on the relevance and availability of policy interventions during recent crises.

Sources include peer-reviewed research, government reports, and official statistics. Rather than generating new empirical data, the study draws from these materials to examine what has worked, what hasn't, and why. The goal is to identify patterns across different contexts and extract practical insights for policy design.

Results and discussions

The war in Ukraine has had devastating effects on small and medium-sized enterprises (SMEs) throughout Eastern Europe. In Ukraine itself, SMEs make up nearly all active businesses—accounting for 99.98% of firms, employing almost three-quarters of the workforce, and contributing around 64% of GDP (UNDP, 2023). But these numbers have changed drastically. The war has pushed production capacity down from 72.4% before the invasion to 45.7% in 2023. Projections suggest a partial recovery to 56% by 2024, though the road ahead remains uncertain (UNDP, 2023).

A synthetic control study (Audretsch et al., 2023) reveals a sharp decline in entrepreneurial activity. Ukraine has lost about 20% of its self-employed workforce—roughly 675,000 individuals. Russia’s SME sector has also taken a hit, with a 42% drop in active firms since the war began, leaving over 1.4 million businesses either closed or severely constrained. These figures underscore the deep, structural damage inflicted by geopolitical conflict on local enterprise.

Beyond Ukraine and Russia, the fallout is being felt across the region. Supply chains have been disrupted. Basic goods—wheat, nickel, platinum—have become harder to move and more expensive to source. As key exporters of these commodities, both Ukraine and Russia played central roles in regional trade. Their absence has driven up prices and injected volatility into the economies of neighboring countries (OECD, 2023).

SMEs have adapted quickly in some cases—relocating operations, moving staff, and reworking logistics. But the uncertainty lingers. Trade remains erratic, investment is hesitant, and support systems are often inconsistent (EBRD, 2023). Recovery will require more than entrepreneurial grit—it will depend on targeted policy choices and coordinated international support.

Government-Backed Financial Support

Access to finance remains one of the biggest hurdles for SMEs in conflict zones. When markets contract, investor confidence falters, and cash flow tightens, firms need outside help to survive. Research confirms that emergency grants, subsidized loans, and credit guarantees can stabilize operations and keep businesses running (Khan et al., 2023).

One example is the European Investment Fund's €1 billion guarantee scheme for SMEs affected by the war in Ukraine. This fund has played a crucial role in maintaining liquidity for firms that might otherwise have folded (Gamage et al., 2020). Poland's own loan program—offering state-backed, low-interest credit to war-affected businesses—has also kept companies afloat during supply chain disruptions (Alatalo, 2024).

Tax relief has helped in other cases. Measures like deferred payments or reduced tax rates offer breathing room for firms under pressure. Caldara and Iacoviello (2022) show how these policies support cash flow and reduce shutdown risk during crises.

Credit guarantees are particularly effective in conflict zones, where private lenders are reluctant to take on risk. By absorbing part of that risk, governments help channel funds to SMEs that would otherwise be locked out of the financial system (Shou et al., 2024).

But financial aid is only as useful as its delivery. Many programs are slowed by bureaucracy or red tape. For SMEs, waiting weeks or months for promised support can mean closing their doors. To address this, some governments have introduced digital disbursement systems and streamlined applications—efforts that make a meaningful difference on the ground (Vasylieva et al., 2024).

Coordination is also key. Isolated efforts—however well-intentioned—are often insufficient. When governments work with development banks, NGOs, and international financial institutions, support is more effective and better targeted. The World Bank's work on SME finance in fragile states offers a useful model for this kind of cooperation (World Bank, 2022).

Finally, support programs must be evaluated. What works in one context may fall short in another. Ongoing assessment helps policymakers adapt, correct mistakes, and scale up successful interventions (Audretsch et al., 2023).

Regulatory Flexibility and Stability

In conflict zones, rules can either help businesses survive—or push them closer to collapse. For SMEs, even small changes in how governments regulate business can have an outsized impact. When institutions allow for flexibility, firms are better able to adapt to fast-changing conditions. When systems remain rigid, administrative burdens grow, and operations stall.

Flexible regulation means more than just emergency exemptions. It involves adjusting bureaucratic processes to reflect the real constraints faced by businesses under stress. During the war, Ukraine streamlined tax filings and accelerated licensing procedures. These changes gave SMEs the ability to operate legally and securely, even as the broader system was under pressure.

Stability is equally important. Entrepreneurs in fragile contexts need to know that the legal framework won't change without warning. Investors, too, depend on predictable contract enforcement and reliable property rights. The EU's Ukraine Facility provided support not only through funding but also by encouraging legal reforms that helped businesses maintain market access in the face of disruption.

Different sectors need different rules. Agriculture, logistics, and digital industries all face distinct regulatory hurdles during conflict. Tailored interventions—such as flexible labor laws or sector-specific tax incentives—can help targeted industries stay viable (Gamage et al., 2020). Estonia's licensing system for remote operations offers one such example. By giving digital entrepreneurs a way to legally operate their businesses while displaced or abroad, Estonia helped protect a crucial part of its economy during periods of uncertainty (Khan et al., 2023).

Still, flexibility comes with risks. Ad hoc rule changes, if not well coordinated, can create confusion or undermine trust. In some cases, short-term regulatory fixes clash with long-term development goals, leading to contradictions that discourage investment. Businesses may hesitate to expand if they believe the legal environment is unstable or politicized.

Institutional capacity is another limitation. In many conflict-affected regions, weak enforcement makes it difficult to implement even the most well-designed reforms. Without adequate oversight, flexible rules can lead to regulatory abuse—whether through corruption, tax avoidance, or market distortion (Audretsch et al., 2023).

For flexibility to work, it must be deliberate and balanced. Policymakers must combine openness to reform with a commitment to legal clarity and accountability. Regulatory stability is not about freezing the system—it's about adjusting with purpose, while protecting the long-term health of the business environment.

Investment in Digital Infrastructure

In conflict zones, digital tools are no longer optional for SMEs—they are vital. In Ukraine, platforms like Diia have enabled firms to handle registration, taxes, and permits remotely, keeping them legally and operationally active during wartime (World Bank, 2022). Estonia's system of remote licensing has offered a similar solution for displaced entrepreneurs.

Basic digital finance tools—mobile banking, payment apps—have replaced disrupted cash systems. These platforms ensure liquidity and reduce exposure to theft or informal credit risks (Gamage et al., 2020). In Lithuania, SMEs have turned to e-commerce to reach external markets, bypassing local instability (Alatalo, 2024).

Still, digital access is uneven. Rural areas often lack infrastructure, and smaller firms face barriers in adopting digital tools. At the same time, cyber threats are growing. Many SMEs remain exposed, with little protection against attacks or data loss (Nasheri, 2023).

Effective digital policy must go beyond access. Security, affordability, and tailored support are essential—especially in fragile economies where digitalisation may be the only way for SMEs to survive.

Supply Chain Adjustment Under Conflict Conditions
Supply chains are among the first systems to collapse in war. For SMEs, this means lost inputs, stalled deliveries, and broken links to markets. In Ukraine and Lithuania, some firms began sourcing locally to cut reliance on cross-border routes (Alatalo, 2024). It hasn't solved the problem, but it's helped maintain partial operations in food production, light manufacturing, and construction.

Border reforms have played a role. Poland and Baltic states temporarily simplified customs to ease movement of goods into and out of Ukraine. These measures reduced delays, but weren't uniform across sectors or regions (World Bank, 2022).

Technology helped where it existed. Shipment tracking, digital invoicing, and warehouse automation gave some firms the ability to react fast. Estonia's digital trade documents reduced paperwork bottlenecks and helped speed up customs processing (Shou et al., 2024).

But the limits are clear. Infrastructure damage and rising costs still block adaptation. Most SMEs can't absorb supply shocks without losing volume or margin. They need working capital, risk-sharing mechanisms, and physical logistics support to cope (Gamage et al., 2020).

Any long-term fix must come through policy. Roads and rail links must be restored, financing adapted to unstable contexts, and rules made simple enough to navigate under pressure (World Bank, 2022).

Cybersecurity and Economic Espionage
As SMEs in conflict zones rely more on digital tools, they face increasing cyber threats. Many operate without basic protection—no IT department, no dedicated security tools, little awareness of risks. This makes them easy targets for phishing, ransomware, and data theft (Gamage et al., 2020).

The risks are not random. Nasheri (2023) shows that state-sponsored cyberattacks often target SMEs in strategic sectors—technology, logistics, manufacturing—especially those with ties to export markets. These attacks aim to disrupt trade, gather intelligence, or destabilize supply chains.

Legal systems in conflict zones often fail to respond. Weak enforcement and unclear frameworks leave firms without recourse when attacked. Caldara and Iacoviello (2022) point out that economic espionage is a growing part of geopolitical competition, and SMEs are exposed but rarely prepared.

Some governments and donors have started responding. ISO standards provide one framework, but most SMEs lack the capacity to implement them. Public-private partnerships and subsidized cybersecurity services have shown promise, but coverage remains uneven (Shou et al., 2024).

Improving cybersecurity in fragile states means more than awareness campaigns. It requires shared infrastructure, affordable digital protection, and policy coordination. Without this, every gain made through digitalisation becomes a new point of vulnerability.

Comparative Cases: SME Policy Responses
Finland offers an example of long-term institutional stability. Public investment in digital systems and cybersecurity has been consistent. The Ministry of Economic Affairs and Employment delivered SME support through grants, research and development vouchers, and training, while Sitra promoted cross-sector innovation, especially in tech and green manufacturing. Administrative

digitalisation—e-tax, digital registries—reduced friction in emergency delivery (Alatalo, 2024; OECD, 2023).

Poland focused on liquidity. The Financial Shield Program, run by the Polish Development Fund, combined grants and loan guarantees for firms facing export losses (World Bank, 2022). While it improved short-term access to finance, implementation issues emerged, including opaque allocation and weak outreach to rural SMEs. Digital uptake has been uneven, particularly outside urban centers (Gamage et al., 2020).

Lithuania pursued local supply resilience and digital adoption. The "Digitize LT" program, supported by EU funds, offered co-financing for digital tools, while new customs corridors with Latvia and Estonia reduced transit delays (Alatalo, 2024). Still, many SMEs lacked the capacity to absorb new systems, pointing to gaps in IT skills and advisory services (Audretsch et al., 2023).

Ukraine operated under emergency conditions. The Diia platform enabled business registration, digital ID, and grants during wartime (Shou et al., 2024). Tax relief, relocation support, and donor-backed financing—mainly from EBRD and USAID—helped maintain basic operations. However, ad hoc interventions lack a long-term recovery framework (Nasheri, 2023; UNDP, 2023).

Across these cases, three factors stand out. First, digital tools are effective only when paired with support and training (Vasylieva et al., 2024). Second, liquidity measures help, but transparency and accessibility determine reach. Third, coordination matters—Finland and Lithuania benefited from institutional alignment, while Poland and Ukraine struggled with fragmentation (Caldara & Iacoviello, 2022; Khan et al., 2023).

Resilience depends not on how many tools exist, but on how they are applied, by whom, and within what institutional conditions.

Conclusion

This paper examined how SMEs manage to operate under the pressure of conflict. The case studies—Finland, Poland, Lithuania, and Ukraine—show how firms adapt when markets shrink, institutions weaken, and uncertainty becomes the norm. What works is not a single policy or funding mechanism, but the alignment of support across several fronts: liquidity, regulation, digital access, trade, and security.

Financial tools—grants, loan guarantees, tax relief—help when they are delivered quickly and transparently. Delays or unclear eligibility rules reduce their effect. In Poland and Ukraine, speed and reach varied, affecting outcomes (World Bank, 2022; Alatalo, 2024). In Finland, funding was more predictable and tied to innovation, not just survival.

Regulation matters too. In war zones, complex rules become impossible to follow. Ukraine cut red tape during the invasion and made licensing and taxes accessible through digital platforms like Diia. That shift helped firms stay operational under fire (Shou et al., 2024).

Digital systems are central. SMEs that could move online—manage payments, file taxes, communicate—stood a better chance. But tech on its own isn't enough. Without cybersecurity, those same tools expose firms to new risks. Most SMEs are unprepared for cyberattacks. Nasheri (2023) shows how economic espionage, often state-backed, targets firms in logistics, tech, and energy. Few have the capacity to defend themselves.

Supply chains remain a major problem. Rerouting takes time. Local sourcing works only if raw materials are available. Lithuania and Estonia moved quickly to set up customs corridors and digitise logistics systems (Shou et al., 2024), but most SMEs lack the cash or staff to adapt at that speed.

Donors and governments need to focus on practical delivery, not just design. Funding must reach the firms that need it most. Digital platforms should come with training, not just infrastructure. Trade corridors work when policies match realities on the ground.

This study has limits. It focuses on Europe, especially Finland and its neighbors. Conflict looks different in Yemen or Sudan. Those contexts require separate analysis. Also, many programs cited here are new. Their long-term effects—on jobs, exports, investment—aren't yet known.

The policy context is changing fast. Cyber threats grow. Climate shocks disrupt logistics. Sanctions reshape regional trade. Policymakers can't rely on one-size-fits-all toolkits. What's needed is coordination: between institutions, across borders, and with the private sector.

SME resilience comes from how policy tools are applied, not how many are available. What matters is fit—between support and need, between institutions and firms, between risk and response.

References

Alatalo, J. (2024). Economic resilience strategies in crisis-prone regions. Journal of Economic Policy Studies, 29(2), 113–130.

Audretsch, D., Momtaz, P. P., Motuzenko, H., & Vismara, S. (2023). The economic costs of the Russia-Ukraine war: A synthetic control study of (lost) entrepreneurship. Journal of Business Venturing Insights, 30(4), 311-334.

Caldara, D., & Iacoviello, M. (2022). Geopolitical risk and the macroeconomy. American Economic Journal: Macroeconomics, 14(1), 1-28.

European Bank for Reconstruction and Development. (2023). The impact of the war in Ukraine on SMEs in Eastern Europe. EBRD Policy Briefs.

Gamage, P., et al. (2020). SME finance in fragile and conflict-affected situations. World Bank Working Paper Series.

Khan, M., Khurshid, A., & Cifuentes-Faura, J. (2023). Geopolitical risks and economic security in Eastern Europe. International Journal of Financial Studies, 11(3), 45-67.

Nasheri, H. (2023). Economic espionage and cybersecurity threats to SMEs. Journal of Cybersecurity Studies, 12(1), 55–72.

Organisation for Economic Co-operation and Development. (2023). Economic resilience and trade disruptions in war-affected regions. OECD Reports.

Quak, E. (2019). Supply chain resilience in conflict-affected areas. Economic Development Journal, 36(4), 78–95.

Shou, Y., et al. (2024). Trade policies and regulatory adaptation during crises. Global Trade Review, 18(1), 22–41.

United Nations Development Programme. (2023). The role of SMEs in economic recovery in post-conflict environments. UNDP Economic Development Reports.

Vasylieva, T., et al. (2024). Digital transformation and economic resilience in war-affected economies. European Economic Review, 75(2), 199–215.

World Bank. (2022). Business environment reforms in fragile states. World Bank Publications.