

CONTESTED GROUND

**Russia's Parallel Engagement in India and
the Risks to Europe's Economic Security**



Executive Summary

India's emergence as the world's fastest-growing major economy has made it a central node in global manufacturing, advanced research, digital infrastructure, and defense production. Europe has responded accordingly, building long-term supply chain, R&D, and defense manufacturing stakes in India. The January 2026 EU–India Free Trade Agreement and accompanying Security and Defence Partnership have now formalized that relationship. Similarly, the UK–India Free Trade Agreement, which entered into force in July 2026, is expected to significantly boost the economic links between the two countries. Russia, meanwhile, is pursuing the same ground.

Isolated from Western markets and technology since its full-scale invasion of Ukraine, Moscow has turned to India to preserve economic resilience and sustain its industrial base. Localized defense production under "Make in India," the routing of Western-origin components through Indian intermediaries, and expanding research and talent collaboration have created structured channels for Russia to circumvent sanctions—all within the same ecosystems where European companies are investing. **European-origin components are already reaching Russian defense entities via Indian supply chains.**

50K+

Strider identified the scale and geographic breadth of this exposure:

Since the start of Russia's full-scale invasion of Ukraine (2022), more than 50,000 sensitive goods, or goods that could potentially have dual-use applicability, reached Russia via India.

At the same time, Russian institutions are recruiting from the same research networks and talent pools that underpin European R&D operations in India. This has been enabled by significantly expanded research collaboration across a broad range of topics between Russian and Indian institutions over the past decade. Co-authored publications increased from 960 in 2017 to 2,300 in 2022, remaining elevated at 2,317 in 2024 and 2,181 in 2025.

As these dynamics deepen, European commercial exposure and economic security risk are becoming impossible to separate. The risks identified in this report do not require governments or businesses to disengage from India. However, the scale and sophistication of Russia's parallel engagement in the same ecosystem demands a more deliberate and structured response. This report concludes by recommending actions leaders in both the public and private sector can take to identify and manage risk within global commercial environments.





India's Strategic Autonomy and Russia's Opening

India's economic scale, expanding innovation base, and integration into global supply chains have made it indispensable to governments and multinational corporations seeking diversification away from both the United States and the People's Republic of China (PRC). European companies increasingly view India as a strategic hedge and long-term manufacturing and R&D hub across aerospace, defense, AI, enterprise software, industrial automation, and advanced engineering.

This trajectory has now been institutionalized. On January 27, 2026, the European Union and India concluded negotiations on a landmark Free Trade Agreement (FTA)—described by European Commission President Ursula von der Leyen as the “mother of all deals”—after nearly two decades of intermittent negotiations. The agreement eliminates or reduces tariffs on over 96% of EU goods exports to India and is projected to double EU exports by 2032, covering sectors including machinery, chemicals, pharmaceuticals, aerospace, and advanced manufacturing.

A parallel Security and Defence Partnership was signed alongside the FTA, deepening cooperation on maritime security, counterterrorism, cyber defense, and defense procurement. Together, these agreements represent the most significant formalization of EU–India strategic and commercial integration to date. The UK, meanwhile, saw its own Free Trade Agreement with India come into effect in July 2026, aiming to significantly boost trade in goods and services between the two countries.

For European and UK companies, these trade deals substantially expand market access and supply chain incentives to anchor operations in India. They also directly increase the stakes of Russia's simultaneous and growing presence within the same industrial and technological ecosystem.

At the same time, New Delhi maintains legacy defense and energy ties with Moscow. India's strategic autonomy doctrine prioritizes flexibility: maintaining engagement across geopolitical blocs while avoiding formal alignment. This posture enables India to expand cooperation with Europe without severing ties to Russia.

For Moscow, this balancing strategy creates opportunity. Russia gains access to:

-  A large and globally connected manufacturing base
-  An advanced and rapidly growing digital ecosystem
-  Expanding research collaboration networks
-  Deep pools of STEM talent
-  Continued indirect exposure to Western technology and capital

Unlike the PRC, whose partnership with Russia has become increasingly asymmetric, India offers Moscow diversification and strategic flexibility. Engagement with India reduces Russia's dependence on Beijing while preserving access to global economic networks.



Exploitation of “Make in India”

“We receive technology from the Russian Federation, adapt it, install it on laptops and PCs and sell it under the Made in India brand.”

Debjit Chakraborty, Director, Russia India Special Interest Group (RISING), in an interview with RBC Press Centre, June 6, 2024.

This statement encapsulates the strategic utility of India’s localization framework for Russia. In a sanctions-constrained environment, adaptation and rebranding under India’s “Make in India” initiative provide a pathway through which Russian technology can be embedded in products manufactured or assembled in India and marketed as Indian output. While structured as legitimate bilateral industrial cooperation, the model reduces the ability to identify place of origin and complicates enforcement of export controls. “Make in India” was designed to transform the country into a global manufacturing hub by incentivizing foreign investment, technology transfer, and domestic production across aerospace, defense, electronics, and advanced manufacturing. For European companies, the initiative offers supply chain diversification and long-term market access. For Russia, it offers insulation.



By embedding industrial activity in India, Russian entities can adapt domestic technologies, integrate them into locally produced systems, and sustain commercial channels into non-Western markets. Localization blurs the line between origin and assembly, particularly in sectors where dual-use components and design architecture are difficult to trace once integrated into complex systems.

Russia’s state-owned defense conglomerate Rostec illustrates this model. Through joint ventures with Indian partners—such as Indo-Russian Rifles Private Limited (a partnership between India’s Ordnance Factory Board and Russian entities under Rostec’s Kalashnikov Concern)—Russia has localized production of small arms in India under the “Make in India” framework. Similarly, Russian-origin munitions, including variants of the 125mm “Mango” armor-piercing tank round, have been produced in India through technology transfer arrangements. These initiatives sustain elements of Russia’s defense industrial base, preserve export channels, and embed Russian-origin systems within India’s domestic production ecosystem.

Defense production highlights the broader structural risk. As European aerospace and defense companies expand localized production in India under the same framework, Russia’s presence within adjacent industrial ecosystems increases exposure. Airbus’s helicopter assembly operations with Tata Advanced Systems and Safran’s joint production of precision-guided munitions with Bharat Electronics Ltd reflect the scale of European integration into India’s defense manufacturing base. These are strategically rational investments. However, they unfold within an environment where Russian actors are simultaneously pursuing technology substitution, supply chain resilience, and alternative export pathways.

The risk for Europe is not direct partnership with Russia, but proximity. Shared subcontractors, co-located suppliers, and overlapping technical domains increase the potential for component diversion, reverse engineering, or economic espionage. Even absent deliberate misconduct, localization reduces transparency across upstream and downstream supply chains, as the RISING statement attests.



Supply Chain Evasion and Technology Access

Beyond localized production, India provides Russia with indirect access to advanced components and dual-use technologies subject to European export controls. Since 2022, India has increased exports to Russia in categories commonly associated with restricted or sensitive goods, including electronics, machinery, precision instruments, transport equipment, metals, and advanced electrical components. A substantial portion of these exports fall within sectors typically targeted by sanctions regimes.

Many of these goods originate in European economies before transiting through Indian intermediaries. This layered trade structure complicates end-use verification and obscures ultimate beneficiaries. Reporting has indicated that Indian entities have supplied advanced computing systems incorporating EU-origin semiconductors to Russian buyers. By routing procurement through India, Russian entities can retain access to high-performance processors and AI-optimized hardware that would otherwise be restricted under direct export controls.

Strider data underscores the scale and geographic breadth of this exposure. Between 2022 and 2025, following Russia’s full-scale invasion of Ukraine, products exported from India to Russia originated disproportionately from advanced European industrial economies:

Table 1: European Origin Countries for Products Exported from India to Russia (2019–2025)

ORIGIN	2019–2021 (3 years, pre-full-scale invasion)	2022–2025 Q1 (3.25 years following full-scale invasion)	% CHANGE
Sweden	151	838	+455%
United Kingdom	625	1,753	+180%
Switzerland	596	1,379	+131%
France	1,272	2,514	+98%
Germany	14,540	9,061	-38%
Czechia	1,646	591	-64%

During this time, there was also a sharp increase in these same types of goods from allied, non-European origin countries to Russian buyers through Indian intermediaries.



Table 2: Allied, Non-European Origin Countries for Products Exported from India to Russia (2019–2025)

ORIGIN	2019–2021 (3 years, pre-full-scale invasion)	2022–2025 Q1 (3.25 years following full-scale invasion)	% CHANGE
Australia	21	132	+529%
United States	2,287	12,792	+459%
Japan	1,620	5,723	+253%
Canada	276	773	+180%

The sharp increase in U.S. (+459%), Japanese (+253%), UK (+180%), Swiss (+131%), and French-origin (+98%) goods highlights the extent to which advanced industrial inputs are flowing into India and subsequently reaching Russia. Even where growth is more modest—or declining, as in Germany’s case—the volume remains significant.

Strider’s supply chain analysis has further identified Indian exporters connected to Russian defense and security-linked entities. These findings suggest that indirect trade routes are not merely commercial anomalies but part of a broader pattern in which sanctioned Russian entities continue to access sensitive components through third-country intermediaries.

Since 2022, more than 50,000 sensitive goods, or goods that could potentially have dual-use applicability, reached Russia via India. For example, French origin carbon fibers reached the Russian company Polymer Company LLC in 2025 via India. Polymer Company LLC has been designated by the Russian government as part of the military-industrial complex and is also a supplier to multiple restricted entities. Carbon fibre materials are used in aerospace, UAVs, missiles, and other defense products.

For European companies operating in India, the risk lies in inadvertent exposure. European-origin components integrated into Indian supply chains may be re-exported onward to Russian end users without the original manufacturer’s awareness. Discovery of such diversion can trigger regulatory scrutiny, financial penalties, and reputational damage—particularly if components are later identified in Russian military systems.

As India deepens its role as a global manufacturing hub, the opacity of complex, multi-jurisdictional supply chains will increase the enforcement burden on European companies. The data in Tables 1 and 2 reinforces a central point: India’s position as a major import hub for Western-origin goods simultaneously enhances its attractiveness to Russia as an intermediary node in Moscow’s sanctions mitigation strategy.



Research Collaboration and Talent Access

Research collaboration between Russian and Indian institutions has expanded significantly over the past decade. Co-authored publications increased from 960 in 2017 to 2,300 in 2022, remaining elevated at 2,317 in 2024 and 2,181 in 2025. This sustained volume indicates that Russia's broader scientific isolation following its full-scale invasion of Ukraine has not materially reduced engagement with India's research ecosystem.

Artificial intelligence represents one of the most strategically significant domains of this collaboration. Since 2022, Russian and Indian universities have signed multiple cooperation agreements identifying AI, advanced computing, and applied data science as priority areas. For example, Chhatrapati Shahu Ji Maharaj University in India and Petrozavodsk State University in Russia formalized cooperation focused on joint AI research and academic exchange.

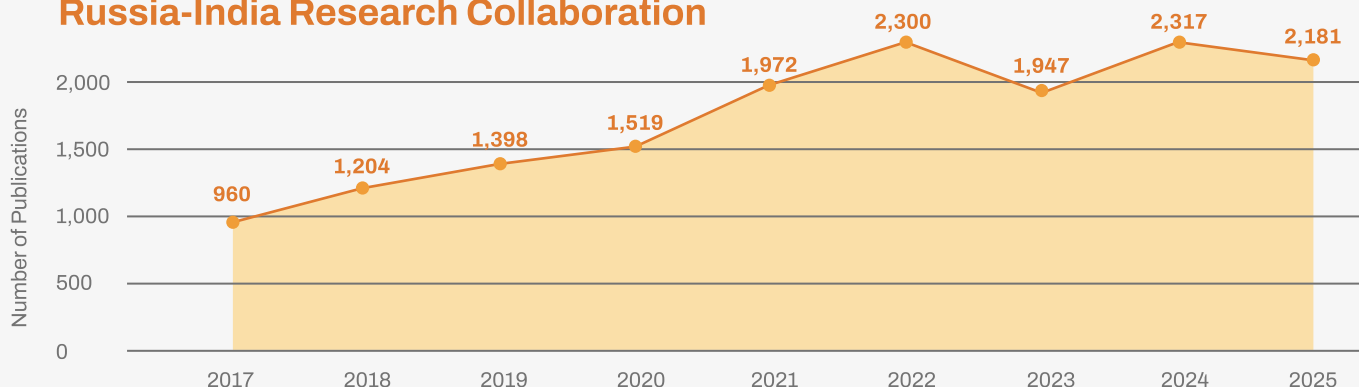
Collaboration on AI development is also occurring outside academia. Russian and Indian researchers and private companies are cooperating on applied AI initiatives, including the joint development of a 'White Paper' aimed at creating a unified framework to assess AI technologies in healthcare and agriculture. While framed as technical coordination, such standard-setting collaboration shapes evaluation methodologies, deployment practices, and performance benchmarking—areas with dual-use implications.

These sectors where Russia-India collaboration is occurring carry strategic sensitivity. AI systems developed for agricultural optimization, health diagnostics, or predictive analytics rely on modeling, data processing, and decision-support capabilities that can be adapted for logistics planning, surveillance analytics, or defense applications. Joint framework development may therefore facilitate methodological and governance-level knowledge exchange beyond narrow sectoral boundaries.

At the same time, India has become a central AI innovation hub for European firms. SAP Labs India—SAP's largest R&D hub outside Germany—plays a major role in AI-enabled enterprise software development. French aerospace and industrial software leader Dassault Systèmes similarly operates an R&D campus in Pune, housing a 3DEXPERIENCE Lab focused on advanced simulation and AI-driven design capabilities for global customers. As European companies anchor advanced R&D activity in India, Russian institutions are simultaneously expanding academic cooperation and recruitment of Indian technical talent to offset domestic labour shortages.

The risk to Europe is not necessarily direct technology transfer from European companies to Russian entities. Rather, it is ecosystem overlap—where shared academic networks, co-authorship, subcontracted research, standards coordination, startup collaboration, and talent mobility create indirect pathways for knowledge spillover. In advanced technology competition, diffusion through shared innovation environments can be as strategically consequential as direct hardware acquisition.

Russia-India Research Collaboration



Strategic Implications for Europe

Russia's engagement with India reflects a deliberate strategy to preserve economic and technological resilience while seeking to avoid overdependence on China. India offers Moscow diversification, global connectivity, and access to talent within an environment deeply integrated with European companies.

For Europe, four structural risks emerge:

01

Export Control Erosion

India's role as a manufacturing and re-export hub increases the probability of diversion of dual-use goods and Western-origin components to Russian defense and intelligence entities. This risk is increasingly acute given the escalating tensions and ongoing conflict between Europe and Russia.

02

Sanctions Evasion

India's position as a major intermediary for European-origin goods creates structured pathways through which sanctioned Russian entities can circumvent export controls. Multi-jurisdictional trade routes and complex re-export arrangements reduce the effectiveness of unilateral and multilateral sanctions regimes.

03

Technology Leakage

Co-location of Russian and European entities within India's defense, aerospace, AI, and digital ecosystems heightens counterintelligence risk and increases opportunities for indirect and direct technology transfer.

04

Talent and Research Spillover

Russian access to Indian research institutions and technical talent may create indirect exposure to European innovation occurring within the same ecosystems.

These risks do not negate the strategic logic of engagement with India. However, it requires calibrated due diligence frameworks, enhanced end-use monitoring, expanded supply chain transparency, and strong alignment between commercial strategy and economic security policy.

India is likely to remain a critical partner for Europe. It is also becoming contested strategic ground. Russia's evolving footprint within India underscores how emerging economies can simultaneously serve as engines of growth and vectors of economic security risk.

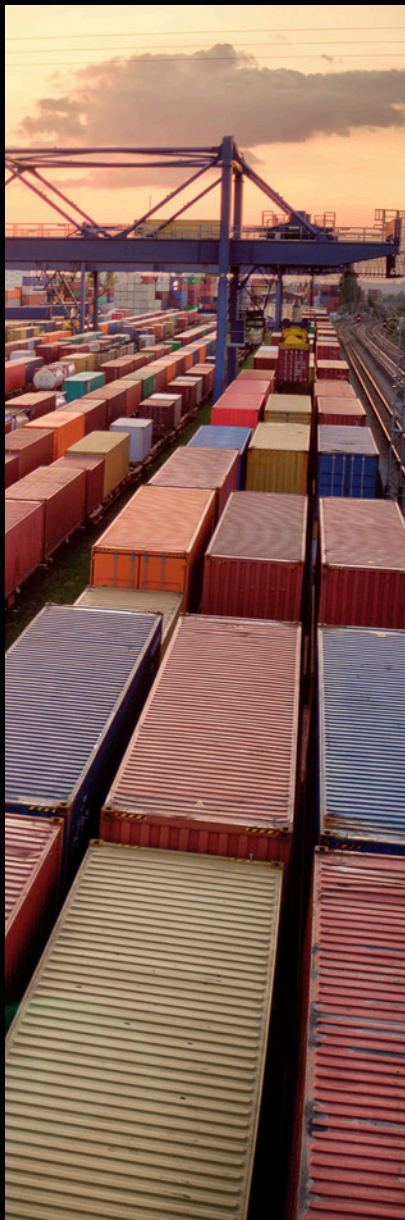


Recommendations

Economic security has emerged as one of the defining challenges of the current geopolitical era. For European governments and businesses, the ability to identify and manage risk within global commercial environments is now as important as traditional defense and intelligence capabilities. India sits at the center of that challenge.

The risks identified in this report do not require governments or businesses to disengage from India. On the contrary, to do so would merely help cement the relationship between Russia and India to the detriment of European economies and geostrategic interests. The EU–India Free Trade Agreement and the associated Security and Defence Partnership represent an opportunity. However, the scale and sophistication of Russia’s parallel engagement in the same ecosystem demands a deliberate and structured response.

The following are opportunities where both public and private sector leaders can manage risks in this space:



For Governments

- **Strengthen multilateral export control coordination.** European governments have an opportunity to work with allies to close the enforcement gaps that allow Western-origin components to reach Russia via Indian intermediaries. This could include harmonizing end-use verification requirements across the EU, sharing intelligence on high-risk Indian entities identified in sanctions-related trade flows, and engaging New Delhi directly on the reputational and diplomatic consequences of continued re-export exposure.
- **Embed economic security provisions within the EU–India and UK–India FTA frameworks.** The EU’s FTA and Security and Defence Partnership, and the UK–India Trade Deal, offer a structural vehicle for raising supply chain transparency standards, establishing joint end-use monitoring mechanisms, and creating bilateral channels for flagging entities of concern. Policymakers have an opening to ensure that economic security considerations are integrated into implementation from the outset, rather than retrofitted after commercial frameworks are established.
- **Develop sector-specific screening frameworks for joint ventures and research partnerships in India.** European governments should consider providing clearer guidance to businesses on which sectors, entities, and research institutions in India carry elevated risk of Russian adjacency and establish a mechanism for flagging joint venture structures that could provide indirect access to controlled technologies.
- **Invest in intelligence on Russia’s India footprint.** The data underpinning this report demonstrates that many of Russia’s activities in India are not covert—they are visible in trade flows, academic publications, corporate filings, and public statements. Governments should consider dedicating resources to monitor and map this footprint on an ongoing basis and share findings with industry through existing economic security outreach programs.





For Businesses

Talent Protection

- Russian organizations operating in India have multiple vectors for recruiting talent and cultivating relationships with employees at European companies—including through academic networks, professional associations, and joint research initiatives. **Businesses should identify which employees and functions are most exposed to these approaches**, particularly those working in dual-use technology domains, advanced R&D, or roles with access to sensitive supply chain data.
- Raising awareness is a primary line of defense. Employees who understand the tactics used to cultivate unwitting relationships—including through seemingly legitimate academic collaboration, conference participation, or professional networking—are far less likely to be drawn into arrangements that create exposure. **Building trust between security teams and technical staff is essential**. Employees who feel informed and respected are more likely to report approaches of concern.
- **Businesses with significant India-based operations should also consider implementing or strengthening an insider threat program**—one equipped with the tools and analytical capabilities to detect early indicators of potential talent or technology loss, including unusual data access patterns, undisclosed external affiliations, or atypical engagement with foreign research institutions.

Third-Party Risk Management

- Third parties—whether suppliers, customers, subcontractors, or research partners—are a business necessity, but they also present a level of risk that must be actively managed rather than assumed away. In the India context, the critical question is not whether a third party has connections to foreign state actors, **but whether those connections are understood and whether appropriate controls are in place**.
- **Businesses should map the connections between their Indian third parties and foreign nation-states**—with particular focus on Russia-linked entities, state-owned enterprises, and institutions identified in sanctions enforcement actions. This mapping should extend beyond direct relationships to second- and third-tier suppliers, where the risk of inadvertent component diversion is highest and visibility is lowest.
- **Awareness of these risks should be raised systematically across internal teams with relevant exposure**—including procurement, legal, compliance, R&D, and business development functions. Economic security risk in India is not solely a compliance matter; it is a commercial and reputational one. Teams that understand the landscape are better positioned to identify anomalies, ask the right questions of partners, and escalate concerns before they become liabilities.