S.F. CUSTOS GLOBAL REACH LTD.
SECURITY · INTELLIGENCE · PROTECTION

SPECIAL REPORT
2026-07-26

STRATEGIC RISK / ADVERSARY COOPERATION / CRITICAL INFRASTRUCTURE

Axis of Pressure: China, Russia, Iran and North Korea as a Coordinated Security Risk

Author: Benjamin Traunecker

Executive summary

The cooperation between China, Russia, Iran and North Korea is no longer a background diplomatic issue. It is becoming a practical security problem for governments, companies and exposed organisations. The four actors do not operate as a single alliance, and their interests still differ. The important shift is narrower and more operational: each actor can now help the others absorb pressure, sustain conflict, test Western response times and widen the number of regions where security managers must plan for disruption.

For companies, the main risk is not that this network produces one coordinated global crisis. The more likely problem is cumulative pressure. A missile supply chain in one theatre, a cyber intrusion against infrastructure in another, maritime disruption in a third, and political signalling elsewhere can combine to stretch attention, insurance capacity, supply chains and crisis-management teams. This is the environment in which travel decisions, site security, executive movement, vendor resilience and evacuation planning must now be judged.

The most exposed organisations are those with regional dependencies in Europe, the Middle East, the Indo-Pacific, the Red Sea, the Gulf, energy markets, defence-adjacent supply chains, critical infrastructure, shipping, aviation, telecommunications and politically visible brands. A company does not need to be the direct target of a state actor to be affected. It may be hit through sanctions exposure, delayed freight, cyber spillover, reduced diplomatic warning time, local protest dynamics or sudden restrictions on movement.

What matters now

The immediate issue is that adversary cooperation reduces the cost of pressure. Russia can sustain its war effort through external supplies and dual-use support. Iran can benefit from military and technical exchange while continuing to pressure regional maritime and proxy environments. North Korea gains hard currency, operational relevance and political cover by supporting Russia. China benefits from a weakened Western focus, access to discounted energy and a wider anti-U.S. diplomatic ecosystem, while avoiding the same level of direct exposure as Moscow or Tehran.

The U.S. intelligence community has publicly assessed that Russia, China, Iran and North Korea are challenging U.S. interests individually and collectively, and that growing cooperation among them increases their resilience and the risk that hostilities involving one could draw in another. NATO has also framed the current threat picture as global and interconnected, with Russia as the most significant direct threat to Allies and with broader linkages between Euro-Atlantic and Indo-Pacific security.

This does not mean every incident should be treated as centrally coordinated. That would overstate the evidence. The more useful assessment is that these actors are building a loose pressure system. It shares capabilities, political messaging, sanctions workarounds, military lessons and distraction effects. The result is a security environment where regional crises travel faster into business risk.

Current operating picture

Russia and North Korea: The clearest operational link is the support North Korea has provided to Russia's war against Ukraine. Public U.S. assessment states that North Korea has sent munitions, missiles and thousands of combat troops to support Russia, tied to the comprehensive strategic partnership announced by Moscow and Pyongyang in June 2024. For European security, this matters because it helps Russia absorb battlefield costs and prolong the war. For companies, the second-order effect is continued pressure on logistics, defence production, insurance, energy pricing and security planning across the NATO eastern flank.

Russia and Iran: Iran has become a military supplier to Russia, especially in unmanned systems. In return, Moscow has offered Tehran military and technical support that can strengthen Iranian weapons, intelligence and cyber capabilities. This linkage matters beyond Ukraine. It can feed back into Middle East risk, including air-defence adaptation, missile development, proxy-network confidence and the ability to threaten maritime chokepoints or regional infrastructure.

China and Russia: China is not fighting Russia's war, but its economic and dual-use support helps Moscow withstand sanctions and sustain combat operations. The China-Russia relationship is the most durable part of the wider network because it sits on trade, energy, diplomatic alignment and defence signalling. Combined military activity, Arctic cooperation and alternative-route planning indicate a relationship that reaches beyond Ukraine. For companies, this raises exposure in shipping, Arctic routes, energy markets, sanctions compliance and technology supply chains.

China, Iran and North Korea: These connections are less uniform but still relevant. China remains central to trade flows, technology access and diplomatic cover. Iran and North Korea both use sanctions workarounds, missile development, cyber activity and asymmetric leverage. Even without a single command structure, the overlap creates a learning environment. Tactics, components, evasion methods and political narratives can move between theatres.

Key risk mechanisms

1. Conflict sustainment: External supplies and dual-use networks make it harder for pressure to force a quick outcome. The practical result is longer wars, longer sanctions regimes and longer business exposure.

2. Technology transfer: Missiles, unmanned systems, electronic warfare, cyber tools and surveillance methods do not need to move openly to change the risk picture. Technical support, components, production methods and battlefield lessons can be enough.

3. Sanctions evasion: The more these actors trade with one another, the more companies face hidden exposure through shipping, intermediaries, components, finance, insurance and beneficial ownership structures.

4. Multi-theatre distraction: A crisis in Ukraine can coincide with pressure in the Gulf, cyber probing against infrastructure, exercises in the Indo-Pacific or political signalling in the Arctic. Security teams then face simultaneous problems with limited staff and attention.

5. Maritime and infrastructure pressure: The Red Sea, the Gulf, energy infrastructure, ports, undersea cables, logistics hubs and aviation corridors are practical pressure points. They affect companies faster than formal diplomatic escalation does.

Early warning indicators

The following indicators would justify a higher organisational alert posture:

- confirmed additional North Korean missile, ammunition or personnel support to Russia;
- public evidence of Russian technical support improving Iranian air-defence, missile, cyber or surveillance capability;

- new China-Russia joint activity in the Arctic, Baltic, Western Pacific or near critical maritime routes;
- sanctions or export-control actions naming intermediaries that touch commercial shipping, electronics, machine tools, telecommunications or energy supply chains;
- attacks or credible threat reporting against maritime traffic in the Red Sea, Gulf of Aden, Strait of Hormuz or Eastern Mediterranean;
- coordinated diplomatic messaging by two or more of the four actors after a major Western policy decision;
- cyber advisories linking state-aligned actors to energy, water, telecoms, transport or financial infrastructure;
- emergency movement notices from embassies, insurers, airlines, port authorities or maritime-security bodies.

Implications for organisations

Executive travel: Senior travel into exposed regions should be approved against current movement conditions, not only country-level risk ratings. The practical questions are airport reliability, route predictability, hotel exposure, protest proximity, medical options and the ability to leave quickly if the local posture changes.

Critical infrastructure and suppliers: Companies dependent on energy, telecoms, ports, shipping, aviation, cloud services or defence-adjacent suppliers should review whether one regional shock could interrupt several functions at once. The risk is not only physical attack. It can be delayed parts, insurance exclusions, unavailable flights, customs disruption or cyber spillover.

Residential and family-office security: High-profile individuals, expatriates and wealthy families may face indirect effects: protest targeting, online exposure, opportunistic crime during local instability, reputational pressure or sudden changes to travel routes. Security plans should include practical household and movement measures, not only strategic monitoring.

Compliance and procurement: Sanctions exposure will remain a moving target. Organisations should look beyond direct counterparties and review logistics providers, payment channels, ownership structures and dual-use components. The weakest point is often a vendor or freight pathway that looked routine before the latest restriction.

Recommended actions

1. **Map exposure by function, not by country.** Identify which executive travel, suppliers, data systems, ports, airports, energy dependencies and insurance terms would be affected by simultaneous pressure in Europe, the Gulf and the Indo-Pacific.
2. **Set watch triggers.** Do not wait for a crisis label. Escalate internal posture when official advisories, maritime alerts, cyber bulletins, embassy notices or sanctions designations cross pre-defined thresholds.
3. **Review movement protocols.** For exposed trips, confirm airport access, driver redundancy, medical contingency, communications backup, safe accommodation and a decision point for cancellation or early departure.
4. **Check sanctions and vendor pathways.** Review shipping, finance, technology and intermediary exposure for links to Russia, Iran, North Korea or sanctioned dual-use networks.
5. **Strengthen basic cyber and infrastructure discipline.** Prioritise multi-factor authentication, VPN exposure review, privileged-account monitoring, supplier access control and incident-response contacts for critical systems.
6. **Prepare a board-level briefing.** Senior leaders should understand that this is not a single-country issue. It is a pressure system that can turn distant military cooperation into local business disruption.

Selected sources

- Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community, March 2025.
- NATO, Washington Summit Declaration, 10 July 2024.
- Foundation for Defense of Democracies, Mark Montgomery analysis on cooperation among China, Russia, Iran and North Korea, July 2026 lead material.
- S.F. Custos Global Reach Ltd., daily cross-source synthesis and special-report candidate pack, 26 July 2026.

Method note

This report is based on open-source material reviewed up to 26 July 2026 and analytical assessment by SF Custos Global. It does not replace legal, insurance, sanctions, medical or country-specific professional advice.