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

SPECIAL REPORT
2026-07-26

STRATEGIC RISK / ADVERSARY COOPERATION / CRITICAL INFRASTRUCTURE

Achse des Drucks: China, Russland, Iran und Nordkorea als koordinierter Sicherheitsrisiko-Komplex

Autor: Benjamin Traunecker

Zusammenfassung

Die Kooperation zwischen China, Russland, Iran und Nordkorea ist kein bloßes diplomatisches Hintergrundthema mehr. Sie entwickelt sich zu einem praktischen Sicherheitsproblem für Regierungen, Unternehmen und exponierte Organisationen. Die vier Akteure handeln nicht wie ein geschlossenes Bündnis, und ihre Interessen bleiben unterschiedlich. Entscheidend ist ein engerer, operativer Punkt: Jeder dieser Akteure kann den anderen helfen, Druck auszuhalten, Konflikte zu verlängern, westliche Reaktionszeiten zu testen und die Zahl der Regionen zu erhöhen, in denen Sicherheitsverantwortliche mit Störungen planen müssen.

Für Unternehmen liegt das Hauptrisiko nicht darin, dass dieses Netzwerk eine einzige koordinierte Weltkrise auslöst. Wahrscheinlicher ist kumulativer Druck. Eine Lieferkette für Raketen oder Munition in einem Kriegsschauplatz, ein Cyberangriff auf Infrastruktur in einem anderen, maritime Störungen in einer dritten Region und politische Drohsignale an anderer Stelle können zusammen Aufmerksamkeit, Versicherungen, Lieferketten und Krisenstäbe überlasten. In diesem Umfeld müssen Reiseentscheidungen, Standortschutz, Bewegungen von Führungspersonen, Lieferantenresilienz und Evakuierungsplanung bewertet werden.

Besonders exponiert sind Organisationen mit Abhängigkeiten in Europa, im Nahen Osten, im Indo-Pazifik, im Roten Meer, im Golf, in Energiemärkten, verteidigungsnahen Lieferketten, kritischer Infrastruktur, Schifffahrt, Luftverkehr, Telekommunikation und politisch sichtbaren Marken. Ein Unternehmen muss nicht direktes Ziel eines staatlichen Akteurs sein, um betroffen zu sein. Es kann über Sanktionen, Frachtverzögerungen, Cyber-Folgewirkungen, verkürzte diplomatische Vorwarnzeiten, lokale Protestdynamik oder plötzliche Bewegungseinschränkungen getroffen werden.

Was jetzt zählt

Der unmittelbare Punkt ist, dass die Kooperation dieser Akteure die Kosten von Druck senkt. Russland kann seine Kriegsführung durch externe Lieferungen und Dual-Use-Unterstützung länger aufrechterhalten. Iran kann von militärischem und technischem Austausch profitieren und zugleich regionale maritime Räume und Proxy-Netzwerke unter Druck setzen. Nordkorea erhält Devisen, operative Relevanz und politische Deckung durch die Unterstützung Russlands. China profitiert von geschwächter westlicher Aufmerksamkeit, vergünstigter Energie und einem breiteren antiamerikanischen diplomatischen Umfeld, ohne sich in gleichem Maß wie Moskau oder Teheran direkt zu exponieren.

Die US-Nachrichtendienstgemeinschaft bewertet öffentlich, dass Russland, China, Iran und Nordkorea amerikanische Interessen einzeln und gemeinsam herausfordern und dass wachsende Kooperation ihre Widerstandsfähigkeit erhöht. NATO hat die aktuelle Bedrohungslage ebenfalls als global und vernetzt beschrieben, mit Russland als bedeutendster direkter Bedrohung für die Alliierten und mit Verbindungen zwischen euro-atlantischer und indo-pazifischer Sicherheit.

Das bedeutet nicht, dass jeder Vorfall zentral koordiniert ist. Eine solche Annahme würde die Beweislage überdehnen. Die bessere Bewertung lautet: Diese Akteure bilden ein loses Drucksystem. Es teilt Fähigkeiten, politische Botschaften, Umgehungswege für Sanktionen, militärische Lernerfahrungen und Ablenkungseffekte. Dadurch wandern regionale Krisen schneller in Unternehmensrisiken hinein.

Aktuelles Lagebild

Russland und Nordkorea: Die klarste operative Verbindung ist die Unterstützung Nordkoreas für Russlands Krieg gegen die Ukraine. Öffentliche US-Bewertungen nennen Munition, Raketen und tausende Kampfkräfte zur Unterstützung Russlands im Zusammenhang mit der im Juni 2024 angekündigten umfassenden strategischen Partnerschaft zwischen Moskau und Pjöngjang. Für die europäische Sicherheit bedeutet das: Russland kann Kosten am Gefechtsfeld länger absorbieren. Für Unternehmen entstehen Folgewirkungen bei Logistik, Verteidigungsproduktion, Versicherungen, Energiepreisen und Sicherheitsplanung entlang der NATO-Ostflanke.

Russland und Iran: Iran ist ein wichtiger militärischer Zulieferer Russlands geworden, insbesondere bei unbemannten Systemen. Im Gegenzug hat Moskau Teheran militärische und technische Unterstützung angeboten, die iranische Waffen-, Aufklärungs- und Cyberfähigkeiten stärken kann. Diese Verbindung reicht über die Ukraine hinaus. Sie kann auf die Risiken im Nahen Osten zurückwirken: Luftverteidigung, Raketenentwicklung, Proxy-Netzwerke und die Fähigkeit, maritime Engpässe oder regionale Infrastruktur zu bedrohen.

China und Russland: China kämpft nicht Russlands Krieg, aber wirtschaftliche und Dual-Use-Unterstützung helfen Moskau, Sanktionen abzufedern und Kampfhandlungen fortzuführen. Die China-Russland-Beziehung ist der dauerhafteste Teil des größeren Netzwerks, weil sie auf Handel, Energie, diplomatischer Abstimmung und militärischer Signalwirkung beruht. Gemeinsame militärische Aktivität, Arktis-Kooperation und Planung alternativer Routen zeigen, dass die Beziehung über die Ukraine hinausreicht. Für Unternehmen erhöht das Risiken in Schifffahrt, Arktisrouten, Energiemärkten, Sanktions-Compliance und Technologie-Lieferketten.

China, Iran und Nordkorea: Diese Verbindungen sind weniger einheitlich, aber relevant. China bleibt zentral für Handelsströme, Technologiezugang und diplomatische Deckung. Iran und Nordkorea nutzen beide Sanktionsumgehung, Raketenentwicklung, Cyberaktivität und asymmetrische Hebel. Auch ohne einheitliche Befehlsstruktur entsteht ein Lernraum. Taktiken, Komponenten, Umgehungsmethoden und politische Narrative können zwischen Schauplätzen wandern.

Zentrale Risikomechanismen

1. Verlängerung von Konflikten: Externe Lieferungen und Dual-Use-Netzwerke erschweren schnelle Wirkung durch Druck. Das praktische Ergebnis sind längere Kriege, längere Sanktionsregime und längere Exponierung von Unternehmen.

2. Technologietransfer: Raketen, unbemannte Systeme, elektronische Kampfführung, Cyberwerkzeuge und Überwachungsmethoden müssen nicht offen verlegt werden, um das Risikobild zu verändern. Technische Unterstützung, Komponenten, Produktionsmethoden und Gefechtsfeld-Erfahrungen können ausreichen.

3. Sanktionsumgehung: Je stärker diese Akteure miteinander handeln, desto stärker steigt für Unternehmen verdeckte Exponierung über Schifffahrt, Zwischenhändler, Komponenten, Finanzierung, Versicherungen und Eigentümerstrukturen.

4. Ablenkung über mehrere Schauplätze: Eine Krise in der Ukraine kann mit Druck im Golf, Cyberaufklärung gegen Infrastruktur, Übungen im Indo-Pazifik oder politischer Signalwirkung in der Arktis zusammenfallen. Sicherheitsteams haben dann mehrere gleichzeitige Probleme bei begrenzter Personal- und Führungskapazität.

5. Druck auf maritime Räume und Infrastruktur: Rotes Meer, Golf, Energieinfrastruktur, Häfen, Unterseekabel, Logistikknoten und Luftverkehrskorridore sind praktische Druckpunkte. Sie treffen Unternehmen schneller als formale

diplomatische Eskalation.

Frühwarnindikatoren

Folgende Indikatoren würden eine erhöhte Organisationsbereitschaft rechtfertigen:

- bestätigte zusätzliche nordkoreanische Raketen-, Munitions- oder Personalunterstützung für Russland;
- öffentliche Hinweise auf russische technische Unterstützung für iranische Luftverteidigung, Raketen, Cyber- oder Überwachungsfähigkeiten;
- neue China-Russland-Aktivitäten in der Arktis, Ostsee, im Westpazifik oder nahe kritischer Seerouten;
- Sanktions- oder Exportkontrollmaßnahmen gegen Zwischenhändler in Schifffahrt, Elektronik, Werkzeugmaschinen, Telekommunikation oder Energie-Lieferketten;
- Angriffe oder glaubwürdige Bedrohungsmeldungen gegen maritime Verkehre im Roten Meer, Golf von Aden, in der Straße von Hormus oder im östlichen Mittelmeer;
- koordinierte diplomatische Botschaften von zwei oder mehr der vier Akteure nach einer größeren westlichen Entscheidung;
- Cyberwarnungen zu staatlich ausgerichteten Akteuren gegen Energie, Wasser, Telekommunikation, Transport oder Finanzinfrastruktur;
- Bewegungswarnungen von Botschaften, Versicherern, Fluggesellschaften, Hafenbehörden oder maritimen Sicherheitsstellen.

Bedeutung für Organisationen

Reisen von Führungspersonen: Reisen in exponierte Regionen sollten anhand aktueller Bewegungsbedingungen freigegeben werden, nicht nur anhand allgemeiner Länderratings. Entscheidend sind Flughafenverfügbarkeit, Routenstabilität, Hotelexponierung, Nähe zu Protesten, medizinische Optionen und die Fähigkeit, bei Lageänderung schnell auszureisen.

Kritische Infrastruktur und Lieferanten: Unternehmen mit Abhängigkeiten von Energie, Telekommunikation, Häfen, Schifffahrt, Luftverkehr, Cloud-Diensten oder verteidigungsnahen Lieferanten sollten prüfen, ob ein regionaler Schock mehrere Funktionen gleichzeitig treffen kann. Das Risiko ist nicht nur ein physischer Angriff. Es kann auch aus verzögerten Teilen, Versicherungsausschlüssen, fehlenden Flügen, Zollstörungen oder Cyber-Folgewirkungen bestehen.

Residential Security und Family Offices: Exponierte Personen, Expatriates und vermögende Familien können indirekt betroffen sein: Protestziele, Online-Exponierung, opportunistische Kriminalität während lokaler Instabilität, Reputationsdruck oder plötzliche Änderungen von Reiserouten. Sicherheitspläne sollten praktische Haushalts- und Bewegungsmaßnahmen enthalten, nicht nur strategische Beobachtung.

Compliance und Beschaffung: Sanktionsrisiken bleiben beweglich. Organisationen sollten über direkte Vertragspartner hinausblicken und Logistikdienstleister, Zahlungswege, Eigentümerstrukturen und Dual-Use-Komponenten prüfen. Die Schwachstelle liegt oft bei einem Lieferanten oder Transportweg, der vor der letzten Beschränkung unauffällig wirkte.

Empfohlene Maßnahmen

1. **Exponierung nach Funktion abbilden, nicht nur nach Land.** Identifizieren, welche Reisen, Lieferanten, Datensysteme, Häfen, Flughäfen, Energieabhängigkeiten und Versicherungsbedingungen durch gleichzeitigen Druck in Europa, im Golf und im Indo-Pazifik betroffen wären.

2. **Beobachtungsauslöser festlegen.** Nicht auf ein Krisenlabel warten. Die interne Sicherheitsstufe sollte steigen, wenn offizielle Warnungen, maritime Meldungen, Cyberhinweise, Botschaftsmeldungen oder Sanktionslisten definierte Schwellen überschreiten.
3. **Bewegungsprotokolle prüfen.** Für exponierte Reisen sollten Flughafenanbindung, Fahrerredundanz, medizinische Ausweichmöglichkeiten, Kommunikationsbackup, sichere Unterkunft und Entscheidungspunkte für Abbruch oder vorzeitige Ausreise bestätigt sein.
4. **Sanktions- und Lieferkettenwege prüfen.** Schifffahrt, Finanzierung, Technologie und Zwischenhändler sollten auf Verbindungen zu Russland, Iran, Nordkorea oder sanktionierten Dual-Use-Netzwerken geprüft werden.
5. **Cyber- und Infrastrukturdisziplin stärken.** Priorität haben Multi-Faktor-Authentifizierung, Prüfung exponierter VPN-Zugänge, Überwachung privilegierter Konten, Lieferantenzugriff und Incident-Response-Kontakte für kritische Systeme.
6. **Briefing für Geschäftsführung oder Board vorbereiten.** Führungskräfte sollten verstehen, dass dies kein Einzelstaatenthema ist. Es ist ein Drucksystem, das entfernte militärische Kooperation in lokale Geschäftsunterbrechung übersetzen kann.

Ausgewählte Quellen

- Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community, März 2025.
- NATO, Washington Summit Declaration, 10. Juli 2024.
- Foundation for Defense of Democracies, Mark-Montgomery-Analyse zur Kooperation zwischen China, Russland, Iran und Nordkorea, Lead-Material Juli 2026.
- S.F. Custos Global Reach Ltd., tägliche Cross-Source-Synthese und Special-Report-Kandidatenpaket, 26. Juli 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.