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

WEEKLY SECURITY BRIEFING
14.-20. Juli 2026

WEEKLY SECURITY BRIEFING · 2026-W30

Weekly Security Briefing

Autor: Benjamin Traunecker

Zusammenfassung für Entscheider — Zentrale globale Entwicklungen dieser Woche

1. **Russlands Personalproblem wurde schwerer zu verdecken.** Das Institute for the Study of War berichtete am 14. Juli unter Verweis auf den ukrainischen Auslandsnachrichtendienst, Russland habe bis Anfang Juli rund 195.000 Vertragssoldaten rekrutiert und damit weniger als die Hälfte des erklärten Jahresziels von 409.000 erreicht. Die ukrainische Militärführung meldete außerdem hohe Verlustkosten für russische Geländegewinne im Oblast Donezk. Entscheidend ist nicht, ob Moskau lokal noch vorrücken kann. Entscheidend ist, dass diese Vorstöße teurer, personalabhängiger und ohne zusätzlichen Rekrutierungsdruck schwerer durchzuhalten werden.

2. **Das Hormus-Risikobild verschob sich von Zwangssignalen zu direkter kommerzieller Exponierung.** ISW und das Critical Threats Project bewerteten am 14. Juli, Iran habe in den vorangegangenen 24 Stunden mindestens drei Handelsschiffe in der Straße von Hormus angegriffen; CENTCOM meldete zugleich Angriffe auf iranische militärische Ziele, die zur Bedrohung der Schifffahrt genutzt worden seien. Mehrere Open-Source-Berichte beschrieben außerdem iranische Behauptungen über Angriffe auf Bahrain, Jordanien und Tanker in der Straße. Die Belege müssen weiter sauber zwischen offiziellen Aussagen, Medienberichten und Analyse getrennt werden, aber die wirtschaftliche Wirkung ist klar: Das Schifffahrtsrisiko im Golf ist nicht mehr theoretisch.

3. **Nordkoreanische Unterstützung für Russland blieb die strategische Verbindung zwischen Europa und Asien.** ISWs Korean Peninsula Update bewertete auf Grundlage ukrainischer Militärnachrichtendienstberichte, Nordkorea liefere einen erheblichen Teil der russischen Artilleriemunition und habe mehr als 600 Artilleriesysteme sowie über 100 ballistische Raketen vom Typ KN-23 und KN-24 bereitgestellt. Es geht nicht nur um Mengen. Das größere Risiko liegt darin, dass ein europäischer Krieg inzwischen mit asiatischen Rüstungs-, Sanktions- und Abschreckungsdynamiken verbunden ist.

4. **Südsudan und Sudan hielten humanitäre Sicherheitsrisiken in Afrika im Vordergrund.** Über ReliefWeb veröffentlichte OCHA-Berichte erklärten, dass zwischen Juni und September 2026 fast 9 Millionen Menschen in Südsudan Nahrungsmittelhilfe benötigen würden, während Konflikt Gemeinschaften weiter vertreibt und humanitäre Operationen stört. Separates Marktmonitoring zu Sudan zeigte einen deutlichen Anstieg des nationalen Minimum Expenditure Basket und der Lebensmittelkosten. Für Organisationen ist das Sicherheitsproblem der Zugang: Konflikt, Krankheit, Lebensmittelpreise und gestörte Hilfe verengen den Raum, in dem Mitarbeitende, Partner und Logistikdienstleister handeln können.

5. **Venezuelas Erdbebenreaktion hielt Lateinamerika im operativen Risikorahmen, auch ohne großen politischen Sicherheitsschock.** ReliefWeb veröffentlichte weiter Material zur Reaktion auf das Erdbeben vom 24. Juni, darunter Karten zu temporären Abfallentsorgungs- und Sortierzentren sowie Lageberichte bis Mitte Juli. Das ist keine Gang-Gewalt-Lage wie Haiti oder Ecuador in früheren Ausgaben. Es ist eine Kontinuitäts- und Infrastrukturfrage: Abfallmanagement, öffentliche Gesundheit, Verkehrszugang und lokale Verwaltungskapazität können nach einer Katastrophe zu Sicherheitsfragen werden.

6. **Cyberrisiko verschob sich zu exponierten Unternehmenssystemen und Zugangsdiebstahl.** BleepingComputer berichtete am 15. Juli, CISA habe Administratoren aufgefordert, aktiv ausgenutzte Schwachstellen in lokalen Microsoft-SharePoint-Servern zu patchen. BleepingComputer berichtete außerdem am 18. Juli, Microsoft beobachte eine Zunahme von ACR-Stealer-Angriffen gegen Unternehmenskunden, bei denen Social-Engineering-Köder, WebDAV und MSHTA eingesetzt würden, um Browser-Passwörter, Authentifizierungstoken und sensible Dokumente zu stehlen. Das Muster ist praktisch: Angreifer zielen auf Systeme, die viele Organisationen noch als normale IT-Infrastruktur und nicht als krisenrelevante Exponierung behandeln.

7. **Maritime Sicherheit vor Somalia blieb aktiv, überholte Hormus aber nicht.** Die Juli-Updates von EUNAVFOR Operation ATALANTA bestätigten weiter Koordinierungsaktivität im westlichen Indischen Ozean, einschließlich früherer Piraterievorfälle vor Somalia und der Befreiung des Massengutfrachters Golden Arsenal nach einem Piratenangriff. Die Einschätzung ist vergleichend. Somalia-bezogene Piraterie bleibt relevant für Routenplanung und Wachhaltung, aber der maritime Druck mit der größten Wirkung liegt diese Woche in der Straße von Hormus.

Lageentwicklung und Einschätzung

Europa HOCH

Russlands kostspielige Vorstöße erhöhen den Rekrutierungsdruck

Russland kann weiterhin offensiven Druck erzeugen, aber die Personalrechnung wird schlechter. Das Institute for the Study of War berichtete am 14. Juli, Rekrutierungsprogramme des russischen Verteidigungsministeriums könnten die Gefechtsverluste nicht ausgleichen. ISW zitierte die Einschätzung des ukrainischen Auslandsnachrichtendienstes, Russland habe bis Anfang Juli 2026 rund 195.000 Vertragssoldaten rekrutiert und liege damit unter der Hälfte des Jahresziels von 409.000. Dieselbe Berichterstattung erklärte, die tägliche Rekrutierungsrate sei von etwa 1.200 Rekruten pro Tag im Jahr 2024 auf etwa 1.090 Mitte 2026 gefallen.

Die Verlustkosten sind wichtiger als eine einzelne tägliche Frontlinie. Der ukrainische Oberbefehlshaber Oleksandr Syrskyi berichtete am 14. Juli, russische Kräfte erlitten mehr als 400 Verluste pro erobertem Quadratkilometer im Oblast Donezk. ISW wies separat darauf hin, dass eigene theaterweite Schätzungen methodisch von Syrskyis oblastbezogener Zahl abweichen. Die Richtung bleibt dennoch konsistent: Russland kauft Gelände weiter mit Personal, nicht mit einem sauberen operativen Durchbruch.

> Intelligence Assessment
> Medium Russland bleibt zu lokalen Vorstößen fähig, aber das Verhältnis zwischen Personalzufluss und Verlustkosten wird zu einer Einschränkung. Die Zuversicht ist mittel, weil die stärksten Zahlen aus ukrainischen Nachrichtendienst- und Kommandoberichten stammen und ISW vor allem den analytischen Rahmen liefert. Die geschäftliche Auswirkung ist ein verlängertes Kriegsrisiko: Sanktionsrisiken, Verteidigungsausgaben, Bahn- und Hafensicherheit sowie Russland-bezogene Gegenparteienprüfung bleiben aktive Planungsthemen.

Für europäische Sicherheitsplanung ist Dauer das Signal. Ein Staat, der weiter in großem Umfang rekrutieren kann, kann offensive Operationen auch dann fortführen, wenn sie ineffizient sind. Das macht die Operation strategisch nicht automatisch tragfähig, verlängert aber den Zeitraum, in dem europäische Regierungen, Unternehmen und Logistikdienstleister unter kriegsbedingter Unsicherheit arbeiten müssen. Kurze Warnzeiten bei Angriffen, Bahnunterbrechungen, Luftverteidigungsaktivität und Sanktionsdurchsetzung gehören weiter zum normalen Umfeld.

Nordkoreanische Munitionslieferungen verstärken dieses Dauerrisiko. ISWs Korean Peninsula Update berichtete auf Grundlage ukrainischer Militärnachrichtendienstinformationen, Nordkorea liefere einen erheblichen Teil russischer Artilleriemunition und habe große Mengen an Artilleriesystemen, Raketen und Granaten bereitgestellt. Das gibt Russland eine externe Unterstützungslinie, die die unmittelbare Wirkung inländischer Produktionsgrenzen reduziert. Zugleich verknüpft es europäische Sicherheitsergebnisse mit Durchsetzungsdruck gegen Nordkorea und mit breiterer US-, südkoreanischer und NATO-Verteidigungsplanung.

AUCH DIESE WOCHE BEOBACHTET

- **Die Qualität russischer Kräfte blieb unter Druck.** ISW berichtete, das russische Verteidigungsministerium habe medizinische und administrative Standards teilweise gelockert und die Rekrutierung von Studierenden, Ausländern und Bewohnern besetzter ukrainischer Gebiete intensiviert. Das kann Zahlen stützen, aber Ausbildung und Disziplin belasten.
- **Sanktionen und Logistik blieben verbunden.** Russische Erdöl-, Transport- und Militärlogistik lassen sich in besetzten und angrenzenden See- und Bahnnetzen schwer trennen. Europäische Unternehmen mit Bezug zu Fracht, Finanzierung, Versicherung oder Schiffseigentum brauchen weiter genaue Due Diligence.

- **Europäische Rüstungsplanung lief im Hintergrund weiter.** Südkoreas wachsende Verteidigungskooperation mit der NATO, die ISW im Korea-Kontext beschrieb, ist für Europa relevant, weil Munition, Schiffbau und Beschaffung inzwischen Teil derselben strategischen Konkurrenz sind.

Naher Osten KRITISCH

Hormus verschiebt sich in direktes kommerzielles Risiko

Die Straße von Hormus ist diese Woche der wichtigste globale Eskalationspunkt. ISW und das Critical Threats Project bewerteten am 14. Juli, Iran habe in den vorangegangenen 24 Stunden mindestens drei Handelsschiffe in der Straße angegriffen. Dieselbe Bewertung erklärte, CENTCOM habe eine weitere Angriffswelle gegen iranische militärische Ziele gemeldet, die zur Bedrohung der Schifffahrt genutzt worden seien. Open-Source-Berichterstattung der Woche trug zudem iranische Behauptungen über Angriffe gegen Bahrain, Jordanien und Tanker, wobei einzelne Behauptungen weiterhin quellenweise eingeordnet werden müssen.

Der Risikomechanismus ist direkte Exponierung unter umstrittener Zuschreibung. Ein Reeder braucht keine vollständige strategische Klarheit, bevor sich Risikobereitschaft verändert. Wenn Handelsschiffe angegriffen werden oder glaubwürdige Stellen unmittelbare Bedrohungsaktivität nahe Hormus melden, reagieren Versicherer, Charterer, Häfen und maritime Verbindungskanäle. Die unmittelbare Folge können höhere Prämien, verzögerte Hafenanläufe, Umroutungen, strengere Meldepflichten und konservativere Schiffsauswahl sein.

> Intelligence Assessment
> Medium Das maritime Risiko im Golf ist für diesen Berichtszeitraum kritisch, weil sich die gemeldete Bedrohung von Signalen zu Angriffen auf Handelsschiffe verschoben hat. Die Zuversicht ist mittel, nicht hoch, weil die Anspruchslage analytische Berichterstattung, offizielle Militärmeldungen und Medienberichte umfasst, die weiter getrennt werden müssen. Die operative Auswirkung ist klar genug: Unternehmen mit Golf-Schifffahrt, Energie-, Luftfahrt-, Executive-Travel- oder regionaler Standortexponierung sollten mit kürzerer Warnzeit und volatileren Routenentscheidungen rechnen.

Auch das politische Signal ist gefährlich. Iran kann Druck über abstreitbare maritime Aktionen, erklärte militärische Antworten, Proxy-Netzwerke und regionale Kommunikation aufbauen. Die Vereinigten Staaten können mit Angriffen, Marinepräsenz und diplomatischem Druck reagieren. Golfstaaten müssen dann Territorium, Luftraum, Hafenzugang und innenpolitische Kommunikation unter hohem Zeitdruck steuern. Diese Mischung erschwert Eskalationskontrolle, selbst wenn kein Akteur einen vollen regionalen Krieg will.

Hisbollah und Libanon bleiben Teil desselben Drucksystems. ISWs Iran-Update vom 14. Juli bewertete, Hisbollah scheine eine Informationsanstrengung zu betreiben, um Entwaffnungsbemühungen der libanesischen Regierung zu verzögern, indem sie einen vollständigen israelischen Rückzug als Vorbedingung darstellt. Das ist kein direktes Hormus-Ereignis, aber es zählt, weil Iran-nahe Netzwerke Teheran mehr als einen Schauplatz für Druck geben. Libanon, Syrien, Irak, Jemen und der Golf bleiben auf derselben Eskalationskarte.

AUCH DIESE WOCHE BEOBACHTET

- **Jemen und das Rote Meer blieben im maritimen Lagebild.** Kein einzelner Rotes-Meer-Vorfall verdrängte Hormus in dieser Ausgabe, aber EUNAVFOR und maritime Quellen hielten den westlichen Indischen Ozean, den Golf von Aden und die Zufahrten zum Roten Meer im Beobachtungsrahmen.
- **Exponierung von Golf-Stützpunkten wurde wichtiger.** Open-Source-Berichte über iranische Behauptungen zu Bahrain und Jordanien sind relevant, weil sie auf möglichen Druck gegen US-nahe militärische Infrastruktur und angrenzende kommerzielle Bewegung hinweisen.
- **Die Sensibilität der Energiemärkte blieb hoch.** Schon eine kurze Phase glaubwürdiger Bedrohung nahe Hormus kann Versicherung und Routenwahl verändern, bevor eine formelle Sperre oder Blockade vorliegt.

Afrika HOCH

Humanitärer Druck und Unsicherheit verengen den Handlungsspielraum

Die belastbarste aktuelle Quellenbasis für Afrika zeigt humanitäre Sicherheitsbeschränkungen statt einer einzigen klaren Gefechtslage. Über ReliefWeb veröffentlichte OCHA-Berichterstattung erklärte, fast 9 Millionen Menschen in Südsudan würden zwischen Juni und September 2026 Nahrungsmittelhilfe benötigen. Dasselbe Update sagte, eskalierender Konflikt vertreibe weiter Gemeinschaften und störe humanitäre Operationen; sechs humanitäre Mitarbeitende seien im Umfeld von Konflikt, Vertreibung und Hilfsoperationen getötet worden. Krankheitsausbrüche, darunter Cholera, erhöhten den Druck zusätzlich.

Sudans Marktdaten zeigen, wie Konflikt zu Zugangsrisiko wird. ReliefWebs Sudan-Marktmonitoring berichtete, der nationale Minimum Expenditure Basket ohne Zuschlag sei gegenüber Mai um 14 Prozent gestiegen, während die medianen Kosten von Nahrungsmitteln um 22 Prozent zunahmen. Besonders hohe Werte wurden unter anderem in Kassala, Nord-Darfur und Süd-Kordofan beobachtet. Diese Zahlen sind nicht nur humanitäre Indikatoren. Sie prägen Sicherheitsverhalten: Diebstahlsrisiko, Mitarbeiterwohl, Gemeindespannungen, Routenwahl und Beschaffungszuverlässigkeit verschlechtern sich, wenn Nahrung und Basisgüter weniger erschwinglich werden.

> Intelligence Assessment
> High Südsudan und Sudan rechtfertigen in dieser Woche ein hohes Afrika-Risiko. Die Zuversicht ist hoch für das humanitäre Zugangsbild, weil es auf OCHA-, ReliefWeb- und Marktmonitoring-Material beruht. Die Sicherheitseinschätzung lautet: Konflikt, Vertreibung, Krankheit und Preisdruck verengen den Handlungsspielraum für NGOs, Auftragnehmer, diplomatische Unterstützungsstrukturen und Unternehmen mit lokalen Partnern.

Das praktische Problem ist Bewegung und Kontinuität. Humanitäre Operationen brechen schrittweise: erst wird Zugang langsamer, dann wird Personal schwieriger, dann geraten medizinische und Lieferannahmen ins Wanken. Für Organisationen sind die Warnzeichen blockierte Straßen, vertriebene Mitarbeitende, bewaffnete Aktivität nahe Hilfsrouten, Treibstoffmangel, Nahrungsmittelpreissprünge und Krankheitsausbrüche nahe Einsatzorten. Keines davon muss ein direkter Angriff auf ein Unternehmen sein, um zum Sicherheitsproblem zu werden.

Der Sahel bleibt hoch, aber bei frischen taktischen Behauptungen quellenbegrenzt. Die Vorprüfung markierte weiter Sorgen über militante Beweglichkeit in Mali, Burkina Faso und Niger, aber aktuelle taktische Behauptungen erreichten durch die verfügbare Quellenbasis keine kundentaugliche Verifikationsschwelle. Die Einschätzung stützt sich deshalb auf etablierte regionale Muster und nicht auf einzelne unbestätigte Vorfälle. Das ist die richtige Disziplin: Eine schwache Behauptung kann Planung verzerren, aber fehlende sofortige Bestätigung macht die Region nicht sicher.

AUCH DIESE WOCHE BEOBACHTET

- **Somalia-bezogenes maritimes Risiko blieb aktiv.** EUNAVFORs Juli-Newsroom hielt Piraterievorfälle und Koordination im westlichen Indischen Ozean im Blick. Somalia zählt sowohl als Land-Sicherheitsproblem als auch als maritimer Beobachtungspunkt.
- **Zentralafrikanische Republik und Madagaskar erschienen in humanitärer Berichterstattung.** ReliefWeb-Beiträge zu Ernährungssicherheit und Länderbriefs hielten diese Staaten im breiteren Afrika-Beobachtungsbild, ohne diese Woche eine eigene Eskalationssektion zu rechtfertigen.
- **Krankheit und Sicherheit von Hilfskräften sind operative Indikatoren.** In Südsudan zählen Cholera und der Tod humanitärer Mitarbeitender, weil sie Evakuierungsannahmen, Feldbesetzung und Partnerzuverlässigkeit beeinflussen.

Asien ERHÖHT

Nordkoreanische Unterstützung für Russland verbindet Europas Krieg mit asiatischer Abschreckung

Nordkoreas Rolle in der Kriegsunterstützung ist zu groß, um sie als Nebenthema zu behandeln. ISWs Korean Peninsula Update vom 14. Juli bewertete unter Verweis auf ukrainische Militärnachrichtendienste, Nordkorea stelle schätzungsweise 25 bis 40 Prozent der aktuellen russischen Artilleriemunition. Dieselbe Berichterstattung erklärte, Nordkorea habe mehr als 600 Artilleriesysteme verschiedener Typen und Kaliber sowie über 100 KN-23- und KN-24-Raketen geliefert, von denen Russland mindestens 80 eingesetzt habe.

Diese Versorgungslinie verändert die Warnlage in zwei Regionen zugleich. Für Europa hilft sie Russland, trotz Verlusten und Sanktionen Feuerkraft aufrechtzuerhalten. Für Asien verschafft sie Nordkorea Einnahmen, militärische Relevanz und Hebelwirkung, während Sanktionsdurchsetzung lückenhaft bleibt. Die Verbindung zieht außerdem Südkorea, NATO, Vereinigte Staaten und Japan enger in ein rüstungsindustrielles Gespräch.

> Intelligence Assessment
> Medium Das Risiko im Indopazifik bleibt erhöht. Die Zuversicht ist mittel, weil die detaillierten Waffenzahlen stark auf ukrainischem Militärnachrichtendienst beruhen, wie ISW ihn darstellt; das breitere Muster militärischer Unterstützung Russlands durch Nordkorea passt jedoch zu etablierter Berichterstattung. Die geschäftlichen Auswirkungen liegen bei Sanktionsprüfung, Verteidigungslieferketten, Schiffahrtskontrollen, Cyberrisiko und Executive-Travel-Annahmen in Nordostasien.

Südkoreas Antwort wird industrieller und strategischer. ISW berichtete, Präsident Lee Jae Myung erweitere die Kooperation mit NATO-Mitgliedern und rahme eine vertiefte Korea-NATO-Verteidigungsindustriepartnerschaft. Seoul strebt außerdem engere verteidigungsindustrielle Zusammenarbeit mit den Vereinigten Staaten an, einschließlich Gesprächen zum Schiffbau. Die Richtung ist klar: Südkorea reagiert nicht nur auf Nordkorea. Es positioniert sich als größerer verteidigungsindustrieller Akteur.

China und Taiwan bleiben im Hintergrund desselben regionalen Risikorahmens. Das stärkste Asien-Signal dieser Woche kam von der koreanischen Halbinsel und der Russland-Nordkorea-Verbindung, aber Taiwan- und Südchinesisches-Meer-Dynamiken bleiben für Lieferketten, Luftraumplanung und maritime Routen relevant. Das Hauptrisiko ist kumulativer Druck statt einer isolierten Krise: mehr militärische Kooperation, mehr Versuche der Sanktionsumgehung und häufigere Abschreckungssignale erschweren normale Geschäftsplanung.

AUCH DIESE WOCHE BEOBACHTET

- **Nordkoreas wirtschaftliche Anreize zählen.** ISW berichtete, Nordkorea habe trotz Sanktionen wirtschaftlich von Waffenverkäufen profitiert. Dieser Anreiz macht künftige Zurückhaltung ohne stärkeren Durchsetzungsdruck weniger wahrscheinlich.
- **Südkoreanischer Schiffbau blieb strategisch relevant.** Seouls Schiffbaukapazität wird Teil US-amerikanischer und alliierter Marineplanung. Das betrifft Verteidigungsbeschaffung, Hafeninfrastruktur und sanktionssensible Industriebeziehungen.
- **Süd- und Südostasien zeigten geringere aktuelle Signaldichte.** Afghanistan, Pakistan, Myanmar und die Philippinen bleiben in den primären Fokusregionen von SF Custos Global, aber die Quellenbasis rechtfertigte diese Woche keine stärkere regionale Eskalationsbewertung.

Lateinamerika / Karibik ERHÖHT

Venezuelas Erdbebenreaktion hält Kontinuitätsrisiko im Fokus

Lateinamerika und die Karibik lieferten diese Woche kein dominierendes Gewaltsignal, aber Venezuelas Erdbebenreaktion bleibt operativ relevant. ReliefWeb veröffentlichte weiter Material zum Erdbeben vom 24. Juni, darunter Karten zu temporären Abfallentsorgungs- und Sortierzentren vom 16. Juli und Hinweise auf Lageberichte bis Mitte Juli. Katastrophenreaktion wirkt auf Papier oft administrativ. In der Praxis betrifft sie Abfall, Gesundheit, lokale Bewegung, kommunale Kapazität, temporäre Standorte und öffentliches Vertrauen.

Das Sicherheitsproblem liegt im Infrastrukturstress nach dem ersten Nachrichtenzyklus. Abfallentsorgungsstellen, beschädigte Gebäude, Wasser und Sanitärversorgung, Verkehrszugang und vertriebene Gemeinschaften können nach dem ersten Erdbebeneinschlag sekundäre Risiken erzeugen. Lokaler Frust kann steigen, wenn Trümmerbeseitigung, Gesundheitsmaßnahmen oder Hilfsverteilung ungleich wirken. Unternehmen und NGOs müssen nicht direkt baulich geschädigt sein, um Störungen zu spüren, wenn Straßen, Unterkünfte von Mitarbeitenden, Auftragnehmer oder öffentliche Dienste betroffen sind.

> Intelligence Assessment
> Medium Das regionale Risiko ist in dieser Ausgabe erhöht statt hoch. Die Zuversicht ist mittel, weil die aktuelle Quellenbasis stärker zu humanitärem und Reaktionsmapping ist als zu verifizierten Sicherheitsvorfällen. Die praktische Auswirkung ist Kontinuitätsplanung: Öffentliche Gesundheit, lokale Verwaltungskapazität, Straßenzugang und Dienstleistungszuverlässigkeit in betroffenen venezolanischen Gebieten müssen weiter beobachtet werden, bevor die Katastrophe aus dem Risikokalender gestrichen wird.

Haiti und Ecuador bleiben hohe Basisrisiken, auch bei dünnerer aktueller Wochensichtung. Frühere UN- und ACLED-Berichterstattung hielt Haitis Gang-Kontrollproblem und Ecuadors organisierte Kriminalität im regionalen Risikobild. Diese Ausgabe wiederholt ältere Vorfalldetails nicht so, als seien sie neu. Sie behandelt beide Länder als stehende Beobachtungspunkte und nutzt Venezuela als stärkste aktuelle Wochenentwicklung.

Das gemeinsame Problem der Region ist begrenzte institutionelle Aufnahmefähigkeit. Ganggewalt, Katastrophenreaktion, Protestdruck und lokaler wirtschaftlicher Stress werden schwerer zu steuern, wenn staatliche Kapazität ungleich ist. Das ist die Verbindung zwischen Haiti, Ecuador, Venezuela und Teilen Mittelamerikas. Der Auslöser unterscheidet sich, aber die geschäftliche Wirkung ähnelt sich häufig: Bewegungsunsicherheit, verzögerte Dienste, höherer Bedarf an geschütztem Transport und weniger vorhersehbare Notfallunterstützung.

AUCH DIESE WOCHE BEOBACHTET

- **Haiti blieb auf der Gang-Gewalt-Beobachtungsliste.** Keine frische aktuelle Quelle verdrängte Venezuela in dieser Ausgabe, aber Zugang in Port-au-Prince, Flughafenverlässlichkeit und lokale Mitarbeitendenbewegung bleiben zentrale Indikatoren.
- **Ecuador blieb ein Beobachtungspunkt für kriminelle Gewalt.** Frühere ACLED-Berichterstattung hielt Gewalt gegen Zivilisten und Hafenstadtexponierung im Fokus. Folge-Daten werden entscheiden, ob Ecuador in der nächsten Ausgabe wieder Hauptabschnitt wird.
- **Peru erschien in erdbebenbezogenem Monitoring.** ReliefWeb- und USGS-bezogenes Material notierte ein Erdbeben der Stärke M5,5 nahe Sicaya, Peru. Das verfügbare Material zeigte keine größere Sicherheitseskalation, gehört aber in die regionale Kontinuitätsbeobachtung.

Cyber / Kritische Infrastruktur HOCH

SharePoint-Ausnutzung und Zugangsdiebstahl rücken Cyberrisiko näher an den Alltag

Die Cyberlage dieser Woche ist direkte Unternehmensexponierung. BleepingComputer berichtete am 15. Juli, CISA habe Administratoren vor aktiver Ausnutzung von drei Schwachstellen in internetexponierten lokalen Microsoft-SharePoint-Servern gewarnt. Der beschriebene Angriffsweg umfasste Authentifizierungsumgehung, Remote-Code-Ausführung, Aktivitäten nach dem Eindringen, Diebstahl von Internet-Information-Services-Maschinenschlüsseln und Persistenz für Malware.

Das ist eine Business-Continuity-Frage, nicht nur eine Patchaufgabe. SharePoint enthält oft operative Dokumente, interne Verfahren, Vertragsmaterial und Personaldaten. Wenn Angreifer Maschinenschlüssel, Persistenz und Zugriff auf internetexponierte Server erhalten, kann der Vorfall von einem Webanwendungsproblem zu Zugangsdatenexponierung, Dokumentendiebstahl und interner Bewegung werden. Das Risiko ist besonders hoch für Organisationen, die ältere lokale Systeme weiter exponieren und zugleich annehmen, Cloud-Migration habe ihre Angriffsfläche reduziert.

> Intelligence Assessment
> High Cyberrisiko ist in dieser Ausgabe hoch, weil die Quellenbasis CISA-bezogene Berichterstattung zu aktiver Ausnutzung einer weit verbreiteten Unternehmensplattform enthält. Die Zuversicht ist hoch für die Existenz aktiver Ausnutzung und mittel bei genauen Exponierungszahlen, weil Internet-Scans Honeypots oder bereits gepatchte Systeme enthalten können. Die wichtigsten Beobachtungspunkte sind Notfallhinweise von Herstellern, öffentliche Ausnutzung, Hinweise auf Zugangsdiebstahl und Belege für laterale Bewegung von exponierten SharePoint-Servern.

Die ACR-Stealer-Berichterstattung weist auf dieselbe Schwachstelle: Zugangsdaten. BleepingComputer berichtete am 18. Juli, Microsoft beobachte eine Zunahme von ACR-Stealer-Angriffen gegen Unternehmenskunden. Die beschriebene Zustellung nutzte ClickFix-artiges Social Engineering, WebDAV-Server und MSHTA, um im Browser gespeicherte Passwörter, Authentifizierungstoken und sensible Dokumente zu stehlen. Das ist kein spektakulärer Angriffstyp. Er wirkt, weil Nutzer, Browser und vertraute Windows-Werkzeuge nahe an wertvollen Zugängen sitzen.

Mehrere sekundäre Cybermeldungen verstärkten das Exponierungsmuster. BleepingComputer berichtete außerdem über öffentliche Exploits für WordPress-bezogene Remote-Code-Ausführungsfehler, eine 7-Zip-Remote-Code-Ausführungsbehebung und Malware gegen macOS-Nutzer über Login-Passwort-Köder. Der gemeinsame Mechanismus ist nicht Neuheit. Angreifer nutzen bekannte Software, öffentlich erreichbare Dienste und Nutzervertrauen, um Persistenz oder Zugangsdaten zu erlangen.

AUCH DIESE WOCHE BEOBACHTET

- **Öffentlich erreichbare Webumgebungen blieben exponiert.** WordPress und andere Content-Plattformen zählen weiter, weil kleine Konfigurationsfehler große Zugangspfade schaffen können.
- **Mac-Umgebungen sind nicht außerhalb des Risikobilds.** Aktuelle Berichterstattung zu macOS-Zugangsdatenködern zeigt, dass Executive- und Kreativteams mit Apple-Geräten weiter Phishing- und Zugangskontrollen brauchen.
- **Ransomware-Druck blieb vorhanden, aber sekundär.** Abbotts Prüfung von Cybervorfällen und ransomwarebezogene Berichte blieben relevant, aber SharePoint-Ausnutzung und Zugangsdiebstahl waren die klareren aktuellen Wochenrisiken.

Globale Einschätzung

Die Woche verbindet Kriegsdauer, maritimen Druck und Unternehmenssysteme. Russlands Rekrutierungslücke beendet den Krieg nicht; sie zeigt, dass Moskau mehr für begrenzte Gewinne zahlt. Irans gemeldete Angriffe auf Handelsschiffe nahe Hormus beweisen keinen vollständigen Schließungsversuch; sie zeigen, wie schnell Golf-Schifffahrt von Routine in Krisenhaltung wechseln kann. SharePoint-Ausnutzung braucht keine geopolitische Großkrise, um Organisationen zu stören, die sensible Inhalte auf exponierten Systemen halten.

Das stärkste überregionale Muster ist Druck auf Zugang. Zugang bedeutet je nach Schauplatz etwas anderes. In der Ukraine geht es um Zugang zu Personal, Munition und Logistikrouten. Im Golf geht es um Zugang zu sicherem Transit und berechenbarer Versicherung. In Südsudan und Sudan geht es um humanitären und personellen Zugang. In Venezuela geht es um funktionierende kommunale Dienste nach einer Katastrophe. Im Cyberraum geht es um Angreiferzugang zu Zugangsdaten und Dokumenten.

Das zweite Muster ist externe Unterstützung, die lokale Krisen verlängert. Nordkoreanische Munition hält russische Operationen aufrecht. Iran-nahe Netzwerke geben Teheran mehrere Eskalationskanäle. Humanitäre Hilfssysteme in Südsudan und Sudan hängen von Finanzierung und Zugang ab, die lokale Konflikte stören können. Cyberangreifer stützen sich auf Standard-Infrastruktur, Social-Engineering-Baukästen und exponierte Dienste. Keines dieser Probleme ist vollständig isoliert.

Das dritte Muster ist verkürzte Warnzeit. Ein neuer maritimer Angriff bei Hormus, eine bestätigte russische Rekrutierungsmaßnahme, ein Cholera-Anstieg in Südsudan, eine öffentliche SharePoint-Ausnutzungswelle oder ein Zusammenbruch venezolanischer Abfallentsorgung können schneller vom Hintergrundthema zum operativen Problem werden, als jährliche Risikozynklen aufnehmen. Organisationen sollten diese Punkte nicht als entfernte strategische Themen behandeln. Es sind Beobachtungsindikatoren mit praktischen Folgen für Bewegung, Kontinuität, Gegenparteien und Datenexponierung.

Quellendisziplin bleibt wichtig. Die stärksten aktuellen Wochenbelege kamen von ISW, OCHA/ReliefWeb, EUNAVFOR, CISA-bezogener Cyberberichterstattung und Microsoft-bezogener Berichterstattung. Sozial- und interviewbasierte Materialien blieben nur früher Kontext und trugen keine kundenseitigen Kernaussagen. Wo Behauptungen aktive Militäroperationen oder iranische Angriffsaussagen betrafen, nutzt die Einschätzung kalibrierte Sprache und behandelt nicht jede Behauptung als abschließend geklärt.

Beobachtungsindikatoren

- CENTCOM-, UKMTO-, EUNAVFOR- oder Golfstaaten-Hinweise, die wiederholte Angriffe auf Handelsschiffe, Schiffsbeschlagnahmen, Minenrisiko oder neue Routenbeschränkungen nahe Hormus, Golf von Oman, Bab el-Mandeb oder Golf von Aden bestätigen.
- Weitere russische Rekrutierungsmaßnahmen, mobilisierungsnahe Regelungen oder lokale Anreizprogramme, die darauf hindeuten, dass die derzeitige Vertragssoldatenpipeline den Gefechtsbedarf nicht deckt.
- Ukrainische, südkoreanische, US-amerikanische oder UN-Berichte, die neue nordkoreanische Raketen-, Artillerie- oder Munitionslieferungen an Russland bestätigen.
- OCHA- oder ReliefWeb-Updates zu weiteren Todesfällen unter Hilfskräften, Konvoi-Zugangsbeschränkungen, Cholera-Ausweitung oder schlechterer Finanzierung in Südsudan.
- Sudan-Marktmonitoring mit weiter steigenden Lebensmittelkorbkosten in konfliktbetroffenen Bundesstaaten, besonders Nord-Darfur, Süd-Kordofan, White Nile und Kassala.
- Venezolanische Katastrophenreaktionsberichte zu Verschlechterung der öffentlichen Gesundheit, Problemen bei Abfallmanagement, Bewegungsbeschränkungen oder Unruhen im Zusammenhang mit Hilfsverteilung.
- CISA-, Microsoft- oder nationale Cyberbehördenhinweise zu Massenausnutzung von SharePoint-Schwachstellen, ACR-Stealer-Kampagnen oder Zugangsdiebstahl gegen Unternehmenskunden.

Abkürzungsverzeichnis

Abkürzung	Bedeutung
ACR	Bezeichnung der Amatera/ACR-Stealer-Malwarefamilie in aktueller Berichterstattung
CISA	Cybersecurity and Infrastructure Security Agency
CENTCOM	United States Central Command
EUNAVFOR	European Union Naval Force
HUR	Hauptverwaltung Aufklärung des ukrainischen Verteidigungsministeriums
ISW	Institute for the Study of War
MSHTA	Microsoft HTML Application Host
OCHA	United Nations Office for the Coordination of Humanitarian Affairs
UKMTO	United Kingdom Maritime Trade Operations

Ausgewählte Quellen

- Institute for the Study of War, "Russian Offensive Campaign Assessment," 14. Juli 2026.
- Institute for the Study of War und Critical Threats Project, "Iran Update Special Report," 14. Juli 2026.
- Institute for the Study of War, "Korean Peninsula Update," 14. Juli 2026.
- OCHA / ReliefWeb, "South Sudan Humanitarian Update (as of 17 July 2026)," veröffentlicht am 18. Juli 2026.
- ReliefWeb, "Sudan | Joint Market Monitoring Initiative (JMMI) Market Overview, 11-20 June 2026," veröffentlicht am 20. Juli 2026.
- EUNAVFOR Operation ATALANTA newsroom updates, Juli 2026.
- BleepingComputer, "CISA warns admins to patch actively exploited SharePoint flaws," 15. Juli 2026.
- BleepingComputer, "Microsoft warns of surge in ACR Stealer attacks on customers," 18. Juli 2026.
- ReliefWeb / MapAction, Venezuela earthquake response mapping and situation-report material, Juli 2026.

Methodische Notiz

S.F. Custos Global Reach Ltd. erstellte dieses Weekly Security Briefing auf Grundlage offen zugänglicher Berichterstattung bis zum 20. Juli 2026. SF Custos Global behandelt offizielle Stellungnahmen, etablierte Nachrichtendienste, UN- und OCHA-Berichterstattung, maritime EU-Quellen, staatliche Cyberhinweise und anerkannte Analyseinstitutionen als primäre Quellenbasis. Social-Media-Behauptungen und interviewbasierter Kommentar werden nur als früher Kontext genutzt, sofern sie nicht durch stärkere Quellen bestätigt sind.