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

WEEKLY SECURITY BRIEFING
29. Juni–5. Juli 2026

WEEKLY SECURITY BRIEFING · KW27 2026

Weekly Security Briefing

Autor: Benjamin Traunecker

Zusammenfassung für Entscheider — Wichtigste globale Entwicklungen dieser Woche

Venezuela durchlebt seine schwerste Naturkatastrophe seit Jahren. ReliefWeb und OCHA berichteten, dass am 24. Juni zwei Erdbeben der Stärke 7,2 und 7,5 die nord-zentrale Region trafen. Bis zum 4. Juli bestätigten die Behörden 2.954 Tote, 16.592 Verletzte, 6.462 Rettungen und mehr als 940 Nachbeben; am stärksten betroffen war der Bundesstaat La Guaira. Das Ausmaß übersteigt die meisten Einzelkatastrophen, die SF Custos Global in diesem Jahr verfolgt hat. Die eigentliche Sicherheitsfolge liegt dabei nicht im Erdbeben selbst, sondern in der Belastung, die es in den kommenden Wochen für Transportwege, medizinische Kapazitäten, örtliche Polizeiarbeit und Hilfsverteilung erzeugt.

Russland fuhr diese Woche eine zweigleisige Kampagne gegen die Ukraine: eine Informationsoffensive rund um Kostjantyniwka und eine tödliche Schlagserie gegen Kyjiw. Das Institute for the Study of War bewertete, dass der Kreml Behauptungen über eine angebliche Einnahme Kostjantyniwkas verstärkte, während russische Kräfte die Stadt tatsächlich zwar infiltriert, aber nicht unter Kontrolle gebracht hatten — zeitlich abgestimmt auf die Telefonate von Präsident Trump mit Wladimir Putin und Wolodymyr Selenskyj am 4. Juli. Unabhängig davon töteten russische Raketen- und Drohnenangriffe auf Kyjiw in der Nacht vom 1. auf den 2. Juli mindestens 17 Menschen und verletzten mehr als 90; Schäden wurden an mehr als 30 Orten registriert. Beide Stränge zusammen zeigen, dass Russland erzählerischen Druck mit fortgesetzter Bereitschaft verbindet, die Hauptstadt direkt anzugreifen.

Der Krieg im Sudan hat einen neuen Brennpunkt. Die Kämpfe verschärften sich um El Obeid, die Hauptstadt des Bundesstaates Nord-Kordofan, wo die Sudanesischen Streitkräfte rund 51 Kilometer Verteidigungswälle und Schützengräben sowie mindestens 14 Kontrollpunkte errichtet haben, während die Rapid Support Forces die Stadt von Westen, Norden und Süden umschließen. Ein hochrangiger UN-Vertreter warnte, das Zeitfenster zur Verhinderung einer größeren Eskalation schließe sich „rasch"; UNICEF berichtete unabhängig davon, dass in den vergangenen sechs Monaten des Krieges mehr als 300 Kinder getötet oder verletzt wurden.

Piraterie ist im Golf von Aden als bestätigte, aktive Bedrohung zurückgekehrt. Die EU-Marineoperation ATALANTA meldete, dass die MV GOLDEN ARSENAL am 1. Juli rund 110 Seemeilen nordöstlich von Bosaso, Somalia, von bewaffneten Männern mit Sturmgewehren und Panzerfäusten angegriffen wurde; eine koordinierte Marinereaktion sicherte das Schiff, Verletzte gab es nicht. ATALANTA bewertete, dass eine Piraten-Aktionsgruppe wahrscheinlich im oder nahe dem international empfohlenen Transitkorridor aktiv ist, neben drei weiteren laufenden Piraterie-Fällen im Somalibecken — eine relevante Verschiebung für jede Organisation, die das Piraterierisiko zugunsten der Houthi-Bedrohungslage zuletzt niedriger gewichtet hatte.

Mit Nordkorea verbundene Akteure weiteten ihre Angriffe auf Software-Lieferketten aus. The Hacker News berichtete unter Berufung auf Recherchen von Socket, dass Akteure aus dem Umfeld der „Contagious Interview"-Kampagne unter der Aktivitätsbezeichnung „PolinRider" 108 bösartige Pakete und Browser-Erweiterungen über npm, Packagist, Go und Chrome veröffentlichten, gezielt gegen Entwickler und Personal mit Kryptowährungsbezug — über gefälschte Bewerbungsverfahren, manipulierte Repositories und schädliche IDE-Aufgaben.

Eine parallele cyberkriminelle Infrastruktur wurde zerschlagen. KrebsOnSecurity und BleepingComputer berichteten, dass FBI, Google und Industriepartner Domains von NetNut beschlagnahmten, einem residentiellen Proxy-Dienst, der mit dem „Popa"-Botnetz verknüpft ist und laut Schätzungen der Google Threat Intelligence Group mindestens zwei Millionen kompromittierte Endgeräte umfasste, die zur Verschleierung krimineller und nachrichtendienstlicher Datenverkehre genutzt wurden.

Kolumbiens Präsidentschaftswahl endete mit einer klaren sicherheitspolitischen Kurswende. Abelardo de la Espriella gewann die Stichwahl mit 49,6 % der Stimmen gegen Iván Cepedas 48,7 %. Er hatte mit einer Ausweitung militärischer Einsätze und engerer Abstimmung mit privaten Sicherheitsdienstleistern gegen den „Total-Peace"-Verhandlungsansatz der scheidenden Regierung geworben — ein Ergebnis, das Organisationen mit Kolumbien-Bezug als wahrscheinliche Verschärfung der Durchsetzungshaltung in den kommenden Monaten lesen sollten.

Europas Bild hybrider Bedrohungen schärfte sich. Das International Institute for Strategic Studies veröffentlichte eine Auflistung von 144 vermuteten Drohnensichtungen im Zusammenhang mit russischen „Schattenflotte"-Schiffen, die zwischen 2024 und 2026 den europäischen zivilen Luftverkehr störten. Das Institut beschrieb die Kampagne als bewusst so kalibriert, dass sie unterhalb der Schwelle bleibt, die eine kollektive NATO-Reaktion auslösen würde — ein Muster, das IISS als Beleg dafür wertete, dass die europäische Luftverteidigung dem aktuellen Bedrohungsumfeld noch nicht gewachsen ist.

Lageentwicklung und Einschätzung

Europa HOCH

Russlands öffentliche Linie zu Kostjantyniwka ist ein nützlicher Indikator dafür, wie Moskau die nächste Verhandlungsphase zu rahmen gedenkt. Das ISW bewertete am 5. Juli, dass Kreml-Vertreter westlichem Publikum eine angebliche russische Einnahme der Stadt präsentierten, unter anderem im Umfeld der Telefonate von Präsident Trump mit Putin und Selenskyj am 4. Juli. Das ISW bewertete zugleich, dass russische Kräfte Teile Kostjantyniwkas infiltriert, die Stadt aber nicht eingenommen hatten, und dass ukrainische Kräfte in Teilen der Stadt weiterhin präsent blieben. Kurzfristige Waffenruhe-Vorschläge rund um umkämpfte Stadtgebiete sollten künftig genau geprüft werden: Sie können humanitär gemeint sein, aber ebenso der militärischen Positionierung und dem Verhandlungsdruck dienen.

> Einschätzung
> Mittel Russland wird voraussichtlich weiter Gefechtsdruck mit Behauptungen verbinden, die auf westliches politisches Publikum zielen, während es zugleich Angriffe auf ukrainische Bevölkerungszentren aufrechterhält. Das Risiko für Unternehmen ist mittelbar, aber real: Sanktionsdebatten, Wiederaufbauplanung, Versicherungsexposition, Logistikrouten und Energieannahmen können alle durch die wahrgenommene militärische Dynamik beeinflusst werden.

Russlands Problem beim Schutz rückwärtiger Gebiete wird sichtbarer. Das ISW berichtete, dass Gazprom eine Vereinbarung mit dem russischen Verteidigungsministerium zur Aufstellung mobiler Feuerbekämpfungsgruppen für Gasinfrastruktur unterzeichnet hat, während russische Freiwilligen- und Militärverbände auch im Zusammenhang mit Drohnenabwehr erörtert wurden — ein Zeichen, dass ukrainische Langstreckenschläge Russland zwingen, Personal und Aufmerksamkeit von anderen Aufgaben abzuziehen.

> Einschätzung
> Mittel Ukrainischer Schlagdruck auf russische Energie- und Logistikziele dürfte ein wiederkehrender Risikofaktor für Unternehmen bleiben. Die unmittelbare wirtschaftliche Wirkung liegt nicht in Geländegewinnen, sondern in der Volatilität von Energieinfrastruktur, Hafen- und Bahnresilienz, Sanktionsdurchsetzung, Versicherungsklauseln und Lieferantenkontinuität.

EBENFALLS BEOBACHTET IN DIESER WOCHE

- **Angriffe auf Kyjiw:** Russische Raketen- und Drohnenangriffe auf Kyjiw in der Nacht vom 1. auf den 2. Juli töteten laut ukrainischen Behörden mindestens 17 Menschen und verletzten mehr als 90; Schäden wurden an mehr als 30 Orten registriert, darunter 20 Wohngebäude und eine medizinische Einrichtung.
- **Drohnenkampagne der Schattenflotte:** Das International Institute for Strategic Studies veröffentlichte einen Bericht mit 144 vermuteten Drohnensichtungen in Europa zwischen 2024 und 2026 und bewertete, dass Russland wahrscheinlich Schattenflotten-Schiffe zum Start von Drohnen nutzte, die wiederholt den zivilen Luftverkehr störten, ohne die Schwelle für eine kollektive NATO-Reaktion zu überschreiten.
- **Vorfall im Fehmarnbelt:** Ein russisches Kriegsschiff, laut Berichten die „Savvy", war am 30. Juni an einem Vorfall im Fehmarnbelt vor der deutschen Küste beteiligt; unabhängig davon bereitet Montenegro die Einführung einer Visumpflicht für russische Staatsangehörige vor — ein Signal verschärfter regionaler Haltung gegenüber Moskau.

Naher Osten ERHÖHT

Die stärkste bestätigte maritime Entwicklung dieser Woche kam von der EU-Marineoperation ATALANTA. ATALANTA meldete, dass die MV GOLDEN ARSENAL am 1. Juli rund 110 Seemeilen nordöstlich von Bosaso, Somalia, von bewaffneten Personen mit Sturmgewehren und Panzerfäusten angegriffen wurde. Die Besatzung setzte Best-Management-Practices um, stoppte das Schiff, löste einen Notrufalarm aus und versammelte sich in der Zitadelle. ATALANTA koordinierte mit den Combined Maritime Forces, der Marine der Republik Korea, der indischen Marine, dem IFC-IOR und regionalen Behörden; das indische Kriegsschiff INS TRIKAND setzte einen Hubschrauber und ein Entertrupp ein, die das Schiff ohne Verletzte sicherten.

Wichtiger als der Einzelvorfall ist ATALANTAs aktuelle Piraterie-Einschätzung: Die Operation erklärte, dass eine Piraten-Aktionsgruppe wahrscheinlich im international empfohlenen Transitkorridor aktiv ist, und verwies auf drei laufende Piraterie-Fälle im Somalibecken mit den Schiffen HONOUR 25, EUREKA und SWARD. Damit rückt Piraterie zurück in die Routenplanung, nachdem viele Betreiber sie über Jahre hinter der Houthi-bezogenen Raketen- und Drohnenbedrohung als nachrangig behandelt hatten.

> Einschätzung
> Hoch Der Golf von Aden und das Somalibecken erfordern jetzt eine doppelte Risikobetrachtung: Piraterie und konfliktbedingte maritime Bedrohungen können im selben Einsatzkorridor zusammentreffen. Für kommerzielle Betreiber ist nicht entscheidend, ob der nächste Vorfall als Piraterie oder als regionale Eskalation eingestuft wird, sondern ob Schiffsprofil, Routenwahl, Besatzungsverfahren und Zugang zu Marinereaktionen die Exposition tatsächlich verringern.

Die öffentliche Vorfallseite von UKMTO zeigte zum Zeitpunkt der Prüfung keine Meldungen. Mehrere Social-Media-Beiträge verwiesen auf mögliche Vorfälle im Roten Meer oder Golf von Aden; diese Angaben wurden in diesem Bericht jedoch nicht

als bestätigte Fakten verwendet, da sie sich zum Zeitpunkt der Prüfung nicht mit der offiziellen UKMTO-Seite abgleichen ließen.

EBENFALLS BEOBACHTET IN DIESER WOCHE

- **Ausweitung der Bodenoperationen Israel-Hisbollah:** Der Juni-Regionalüberblick von ACLED verzeichnete einen Anstieg der israelisch-hisbollahnahen Angriffe im Mai um rund 10 % gegenüber dem Vormonat; israelische Kräfte drangen nördlich des Litani-Flusses in den Distrikt al-Nabatieh vor und weiteten ihre Bodenpräsenz um den Beaufort-Grat und das Wadi Saluki aus — eine langsamer verlaufende Eskalation, die deutlich weniger Berichterstattung erhielt als die Gaza- und Iran-Stränge.
- **Innerer Riss im Jemen:** Die Houthis haben Angriffe auf die Rotmeer-Schifffahrt seit dem Gaza-Waffenstillstand weitgehend eingestellt, doch ist ein neuer Riss zwischen Saudi-Arabien und den Vereinigten Arabischen Emiraten entstanden — über eine mögliche Neuaufteilung Jemens und über die Führung südlicher Kräfte, die jemenitische Ölfelder besetzt haben. Ein Streit mit unmittelbarer Bedeutung für den Zugang zum Energiesektor im Süden Jemens.
- **Reibung bei der Hormus-Umsetzung:** Streitigkeiten über die Umsetzung des US-iranischen Memorandums spielten sich am sichtbarsten weiter rund um die Straße von Hormus ab; das Rahmenabkommen soll die Feindseligkeiten nur vorübergehend aussetzen und die Straße wieder öffnen, während Irans Nuklearprogramm und eine langfristige Sanktionserleichterung aufgeschoben bleiben.

Afrika HOCH

Der Fall GOLDEN ARSENAL bestätigt, dass die maritime Bedrohung am Horn von Afrika aktiv ist. Der Vorfall zeigt zugleich, dass Besatzungsdisziplin und Marinekoordination eine erfolgreiche Kaperung weiterhin verhindern können, wenn Meldungen rechtzeitig erfolgen und BMP-MS-Maßnahmen befolgt werden — ein Hinweis darauf, dass die Reaktionskette funktioniert, sofern sie früh genug ausgelöst wird, nicht ein Grund, das Risiko herabzustufen.

> Einschätzung
> Hoch Somalische Piraterie ist für Schiffe in der Nähe des IRTC und des Somalibeckens kein nachrangiges Hintergrundrisiko mehr. Das aktuelle Muster bleibt beherrschbar, aber nur, wenn Reedereien davon ausgehen, dass bewaffnete Gruppen über ausreichende Reichweite verfügen, um Zitadellenverfahren und Marinereaktionen zu erzwingen.

Open-Source-Social-Media-Kanäle berichteten von Kämpfen um Anéfis in Mali und möglichen Verlusten auf malischer und russisch-naher Seite. Das Material war spezifisch genug, um eine Beobachtung zu rechtfertigen, wurde jedoch bis Redaktionsschluss durch offizielle, Agentur-, NGO- oder etablierte Analysequellen, die während dieser Recherche verfügbar waren, nicht unabhängig bestätigt und sollte unterhalb der Schwelle für eine feste mandantenseitige Tatsachenaussage bleiben.

> Einschätzung
> Niedrig Die Sahelzone bleibt strukturell hochriskant, doch die Berichterstattung zu Anéfis dieser Woche sollte als Hinweis, nicht als bestätigter Sachverhalt behandelt werden. Beobachtungspunkt bleibt, ob JNIM, FLA-nahe oder andere bewaffnete Akteure den Druck auf militärische Bewegungskorridore im Norden und Zentrum Malis aufrechterhalten.

EBENFALLS BEOBACHTET IN DIESER WOCHE

- **Sudan — Belagerung von El Obeid:** Die Kämpfe verschärften sich um El Obeid, die Hauptstadt Nord-Kordofans, wo die Sudanesischen Streitkräfte die Stadt mit rund 51 Kilometern Wällen und Gräben sowie mindestens 14 Kontrollpunkten befestigt haben, während die Rapid Support Forces sie aus drei Richtungen umschließen. Ein hochrangiger UN-Vertreter warnte, das Zeitfenster zur Verhinderung einer größeren Eskalation schließe sich; UNICEF berichtete von mehr als 300 im Krieg der vergangenen sechs Monate getöteten oder verletzten Kindern.
- **Nigeria — Schulentführung:** Bewaffnete überfielen die Lassa Day Secondary School im Gebiet Askira-Uba im Bundesstaat Borno und entführten 25 Mädchen, 11 Jungen und drei Lehrkräfte, inmitten verstärkter nigerianischer Militäroperationen gegen Boko Haram und die Islamic State West Africa Province im Tschadseebecken.
- **DR Kongo — Ressourcenabfluss:** Ein neuer UN-Bericht stellte einen zunehmenden Goldschmuggel aus der kongolesischen Provinz Ituri nach Uganda fest; die Lücke zwischen Ugandas gemeldeten Goldexporten und der eigenen Förderung lässt sich zunehmend durch geschmuggeltes kongolesisches Material erklären — ein langsamer verlaufendes Governance-Risiko mit unmittelbarer Bedeutung für Sorgfaltsprüfungen in Lieferketten und bei Sanktionsexposition.

Asien ERHÖHT

The Hacker News berichtete unter Berufung auf Recherchen von Socket, dass mit Nordkorea verbundene Akteure aus dem Umfeld der „Contagious Interview"-Kampagne im Rahmen von „PolinRider" 108 einzigartige Pakete und Browser-Erweiterungen über npm, Packagist, Go und Google Chrome veröffentlichten. Die Aktivität soll laut Bericht 162 bösartige Release-Artefakte, schädliche JavaScript-Loader, gezielte Ansprache von Entwicklern, kompromittierte Maintainer-Zugänge und Ausführung über Entwicklertools wie VS-Code-Task-Dateien umfassen.

Die Zielsetzung ist eindeutig. Entwickler, im Kryptobereich Tätige und Maintainer sind attraktiv, weil ihre Rechner persönliches Vertrauen, Code-Repositories und Produktivumgebungen miteinander verbinden. Ein manipuliertes Paket muss keine Firewall durchbrechen, wenn es einen Entwickler dazu bringen kann, das falsche Projekt zu installieren, zu testen oder zu öffnen.

> Einschätzung
> Mittel Mit Nordkorea verbundene Angriffe auf Software-Lieferketten dürften ein wiederkehrendes Unternehmensrisiko bleiben, weil sie Einstellungsverfahren, Freelancing und Entwicklervertrauen ausnutzen und nicht nur Schwächen am Netzwerkrand. Am stärksten exponiert sind Organisationen mit schnell wachsenden Entwicklerteams, schwacher Paket-Governance oder Zugängen mit Kryptowährungsbezug.

EBENFALLS BEOBACHTET IN DIESER WOCHE

- **Taiwanstraße — ruhigerer Monat:** Taiwans Verteidigungsministerium verzeichnete im Juni 12 Tage ohne Vorstöße der Volksbefreiungsarmee über die Mittellinie der Taiwanstraße — eine Rückkehr zum Niveau vor 2024, nachdem sich die PLA-Aktivität nach der Amtseinführung von Präsident Lai 2024 etwa verdoppelt hatte. Ein Deeskalationssignal, das beobachtet, aber nicht vorschnell als Trend gewertet werden sollte.
- **Präsenzaufbau am Scarborough-Riff:** Ein chinesisches Küstenforschungsschiff, die Tong Ji, fuhr kurz nach der Entfernung einer dortigen Plattform zum Scarborough-Riff — im Einklang mit dem bewerteten Muster, dass Peking eine dauerhaftere oder halbdauerhafte bemannte Präsenz aufbaut, um seinen Gebietsanspruch zu untermauern.
- **Trägerrotationen:** Der chinesische Flugzeugträger Liaoning kehrte am 23. Juni nach einem über 40-tägigen Einsatz im Südchinesischen Meer und im westlichen Pazifik in seinen Heimathafen Qingdao zurück, während der Träger Fujian weiterhin die Taiwanstraße durchquerte — Aktivität im Einklang mit häufigeren Trägerrotationen zwischen den Theaterkommandos der PLA.

Lateinamerika / Karibik HOCH

ReliefWeb/OCHA berichtete, dass Venezuela nach zwei Erdbeben der Stärke 7,2 und 7,5, die am 24. Juni die nord-zentrale Region trafen, einen nationalen Notstand erlebte. Bis zum 4. Juli meldeten die Behörden 2.954 Tote, 16.592 Verletzte, 6.462 Rettungen, mehr als 940 Nachbeben und rund 16.309 Menschen, die ihr Zuhause verloren hatten; am stärksten betroffen war der Bundesstaat La Guaira. Das UN-System und Partnerorganisationen reagierten in Abstimmung mit der Regierung mit sektorübergreifender Unterstützung.

> Einschätzung
> Hoch Venezuelas Erdbebennotstand ist ein schwerer humanitärer und operativer Schock. Die nächste Risikophase wird durch Nachbeben, Unterkunftskapazitäten, medizinische Belastung, Straßenzugang und die Fähigkeit des Staates bestimmt, Hilfsverteilung zu steuern, ohne die lokale Sicherheitslage zu verschärfen.

Der Nachrichtenstrom von InSight Crime führte diese Woche Analysen und Profile zu den mexikanischen Ardillos, dem kolumbianischen Chiquito Malo und dem venezolanischen Larry Changa sowie einen Beitrag zu Mexikos kriminellen Druckpunkten: Drogen, Korruption und CJNG-Treibstoffdiebstahl. Haiti bleibt ein schwerwiegendes Sicherheitsproblem; Social Media und Fachkommentare verwiesen erneut auf Bandenkontrolle und eingeschränkte Bewegungsfreiheit in Port-au-Prince, wobei die kursierenden konkreten Zahlen bis Redaktionsschluss nicht unabhängig bestätigt waren.

> Einschätzung
> Mittel Der Druck organisierter Kriminalität in Lateinamerika ist kein Ein-Länder-Problem. Der gemeinsame Mechanismus ist kriminelle Kontrolle über Infrastruktur, Gefängnissysteme, Treibstoffflüsse, Häfen, Zugang zu Wohnvierteln und lokalen politischen Schutz. Für Unternehmen zeigt sich die Exposition in Routenstörungen, Erpressungsrisiko, unzuverlässigen lokalen Auftragnehmern und plötzlichen Änderungen der Strafverfolgungshaltung.

EBENFALLS BEOBACHTET IN DIESER WOCHE

- **Wahlergebnis in Kolumbien:** Abelardo de la Espriella gewann die Stichwahl um das kolumbianische Präsidentenamt mit 49,6 % der Stimmen gegen Iván Cepedas 48,7 %. Er warb mit einer Ausweitung militärischer Einsätze und engerer Abstimmung mit privaten Sicherheitsunternehmen gegen den scheidenden „Total-Peace"-Ansatz — ein Ergebnis, das die Durchsetzungshaltung gegenüber bewaffneten Gruppen in den kommenden Monaten voraussichtlich verschärft.
- **Sicherheitsaufgebot Mexikos zur Weltmeisterschaft:** Mexiko hat für die FIFA-Weltmeisterschaft 2026, die vom 11. Juni bis 19. Juli läuft und rund 5,5 Millionen internationale Besucher erwarten lässt, knapp 100.000 Militär- und Bundespolizeikräfte in den Austragungsstädten eingesetzt — eine konzentrierte Sicherheitsoperation mit unmittelbarer Bedeutung für jede Organisation, die während des Turnierfensters Personal durch Austragungsstädte bewegt.
- **Spannungen zwischen Ecuador und Kolumbien:** Grenzspannungen zwischen Kolumbien und Ecuador, einschließlich eines früheren Handelsstreits zwischen beiden Regierungen, erschweren weiterhin Bemühungen um eine engere Sicherheitskooperation an gemeinsamen Grenzgebieten, die von Netzwerken organisierter Kriminalität genutzt werden.

Globale Cybersicherheit / Kritische Infrastruktur HOCH

KrebsOnSecurity berichtete am 2. Juli, dass das FBI mit Industriepartnern zusammenarbeitete, um Hunderte Domains zu beschlagnahmen, die mit NetNut verbunden sind — einem residentiellen Proxy-Dienst, den Sicherheitsfirmen mit dem Popa-Botnetz in Verbindung bringen. Krebs zitierte Berichte der Google Threat Intelligence Group, wonach NetNut breit weiterverkauft und von cyberkriminellen sowie nachrichtendienstlichen Gruppen genutzt wurde, um Quell-IP-Adressen zu verschleiern, auf Opferumgebungen zuzugreifen und Password-Spraying-Angriffe durchzuführen. BleepingComputer

berichtete, dass Google das Netzwerk auf mindestens zwei Millionen kompromittierte Geräte schätzte, darunter Smart-TVs und Streaming-Boxen, und dass Google, das FBI, Lumen, Shadowserver und weitere Partner an der Zerschlagung beteiligt waren.

> Einschätzung
> Hoch Die Zerschlagung von NetNut/Popa dürfte kriminelle Kapazitäten kurzfristig verringern, doch das Proxy-Ökosystem ist widerstandsfähig. Betreiber können Ersatzkapazität kaufen, Zugänge weiterverkaufen und zu anderen Anbietern wechseln. Sicherheitsteams sollten mit einer Abschwächung, nicht einem Verschwinden des durch residentielle Proxys ermöglichten Missbrauchs rechnen.

Die Berichterstattung zum nordkoreanisch verbundenen PolinRider überschneidet sich mit diesem Bild. Bösartige Pakete, Browser-Erweiterungen, IDE-Aufgaben und manipulierte Repository-Historien machen die Entwicklungsumgebung selbst zur Zielumgebung — besonders für Unternehmen, die auf Code-Abhängigkeiten Dritter, schnelle CI/CD-Prozesse oder Auftragnehmer mit weitreichendem Repository-Zugang angewiesen sind.

> Einschätzung
> Mittel Angriffe auf Software-Lieferketten bleiben attraktiv, weil sie Vertrauen in Zugang verwandeln. Die nächsten nützlichen Indikatoren sind bösartige Paket-Cluster, ungewöhnliches Verhalten von Maintainer-Konten, versteckte IDE-Ausführungsaufgaben und Post-Install-Skripte, die externe Infrastruktur kontaktieren.

Globale Einschätzung

Die Woche hat keinen einzelnen globalen Schock hervorgebracht, der alle anderen Risiken überlagert. Sie hat jedoch ein klareres Bild davon gezeichnet, wie sich mehrere Risikosysteme inzwischen überlagern. Russland versucht, Gefechtsnarrative in diplomatischen Druck zu verwandeln, während es zugleich ukrainische Städte direkt angreift, und seine Schattenflotten-Drohnenkampagne zeigt dieselbe Logik kalibrierten Drucks im europäischen Luftraum. Maritime Betreiber im Golf von Aden müssen Piraterie wieder einkalkulieren, ohne das Konfliktumfeld im Roten Meer oder die langsamer verlaufende Eskalation Israel-Hisbollah nördlich des Litani aus dem Blick zu verlieren. Cyberakteure nutzen private Endgeräte, Paket-Repositories und Entwicklervertrauen als Infrastruktur, weitgehend unabhängig von einem einzelnen geopolitischen Krisenherd. Der Krieg im Sudan und das Erdbeben in Venezuela zeigen zwei sehr unterschiedliche Wege zum selben Ergebnis: staatliche Kapazität, die mit dem Ausmaß der Krise nicht Schritt hält. Lateinamerika fügt eine dritte Ebene hinzu — organisierte Kriminalität, eine Wahl, die die Durchsetzungshaltung voraussichtlich verschärft, und ein Großsportereignis mit einem historischen Sicherheitsaufgebot, alles innerhalb derselben Berichtswoche.

Für Unternehmen liegt die eigentliche Herausforderung in der Verdichtung von Risiken. Sicherheitsentscheidungen müssen zunehmend mehrere Risikomechanismen gleichzeitig berücksichtigen: Ein Schiff kann in ein und demselben Korridor Piraterie- und Konfliktrisiko zugleich ausgesetzt sein; ein Entwicklerlaptop kann zum Einfallstor in die Produktivumgebung werden; eine Naturkatastrophe kann zu einem Mobilitäts-, Unterbringungs- und Ordnungsproblem werden; eine Behauptung vom Schlachtfeld kann Sanktionen, Versicherungen und politische Annahmen beeinflussen, bevor die Faktenlage gesichert ist; ein Wahlergebnis kann die Durchsetzungshaltung schneller verändern als jeder einzelne Vorfall.

Die stärksten bestätigten Signale dieser Woche sind OCHAs Daten zum Erdbeben in Venezuela, der ATALANTA-Bericht zur MV GOLDEN ARSENAL, UN-Berichterstattung zur Belagerung von El Obeid, die Berichte von KrebsOnSecurity und BleepingComputer zu NetNut/Popa, die Berichterstattung von The Hacker News zu den nordkoreanisch verbundenen bösartigen Paketen sowie das zertifizierte Wahlergebnis in Kolumbien. Die schwächsten Signale sind die aktuellen Social-

Media-Behauptungen zu Mali dieser Woche und unbestätigte Vorfallmeldungen zum Roten Meer. Sie bleiben nützliche Beobachtungspunkte, sollten aber ohne weitere Bestätigung keine Entscheidungen leiten.

Kurzfristige Beobachtungspunkte: weitere ATALANTA- oder UKMTO-Meldungen nahe dem IRTC; Hinweise auf weitere Aktivität von Piraten-Aktionsgruppen; ob die Verteidigungslinien von El Obeid halten oder durchbrochen werden; ukrainische Langstreckenschläge gegen russische Energie- oder Logistikziele sowie weitere russische Angriffe auf Kyjiw; bösartige Paket-Cluster mit Bezug zu Entwicklertools; und bestätigte Änderungen des humanitären Zugangs in Venezuela.

Frühwarnindikatoren

- **Kostjantyniwka und Waffenruhe-Signale:** jeder formelle Waffenruhe- oder humanitäre Korridorvorschlag mit Bezug zur Stadt, und ob dieser mit fortgesetzten russischen Angriffen andernorts in der Ukraine zusammenfällt.
- **Tempo der Piraterie im Somalibecken:** weitere ATALANTA-, UKMTO- oder EUNAVFOR-Meldungen zu Vorfällen oder Sichtungen von Piraten-Aktionsgruppen nahe dem international empfohlenen Transitkorridor in den nächsten zwei bis drei Wochen.
- **Verteidigungsperimeter von El Obeid:** satelliten- oder agenturgestützte Bestätigung, ob die Wall- und Kontrollpunktlinie der Sudanesischen Streitkräfte hält, durchbrochen oder aufgegeben wird, sowie jede UN-Erklärung, die von Warnsprache zu bestätigter Berichterstattung über Gräueltaten übergeht.
- **Kompromittierungs-Cluster bei Entwicklertools:** neue Sperrungen oder Warnmeldungen zu npm-, Packagist-, Go- oder Chrome-Paketen mit Bezug zur PolinRider-Infrastruktur, Missbrauch von IDE-Task-Dateien oder Anwerbeköder im Rahmen von „Contagious Interview".
- **Nachbeben- und Zugangsdaten Venezuela:** Aktualisierungen der OCHA-Lageberichte, ob sich Todes- und Verletztenzahlen stabilisieren und ob Straßen-, Hafen- und Flughafenzugang wiederhergestellt oder weiter beeinträchtigt wird.
- **Sicherheitspolitischer Übergang in Kolumbien:** konkrete Ankündigungen der künftigen Regierung de la Espriella zu militärischen Einsatzstärken, Abstimmung mit privaten Sicherheitsdiensten oder dem Status der auslaufenden „Total-Peace"-Verhandlungen mit bewaffneten Gruppen.
- **Vorfälle im Fehmarnbelt und in der Ostsee:** weitere Berichterstattung zu russischer Marineaktivität in den Ostsee-Zufahrten, und ob weitere Staaten dem Vorgehen Montenegros bei strengeren Visa-Beschränkungen für russische Staatsangehörige folgen.

Glossar der Abkürzungen

Abkürzung	Bedeutung
ATALANTA	EU-Marineoperation ATALANTA
BMP-MS	Best Management Practices for Maritime Security
CJNG	Cártel Jalisco Nueva Generación
GTIG	Google Threat Intelligence Group
IISS	International Institute for Strategic Studies
IRTC	International Recommended Transit Corridor
ISW	Institute for the Study of War
JNIM	Jama'at Nusrat al-Islam wal-Muslimin
OCHA	UN-Büro für die Koordinierung humanitärer Angelegenheiten
PAG	Piraten-Aktionsgruppe

Abkürzung	Bedeutung
PLA / PLAN	Volksbefreiungsarmee / Marine der Volksbefreiungsarmee
RSF	Rapid Support Forces (Sudan)
SAF	Sudanesische Streitkräfte
UKMTO	United Kingdom Maritime Trade Operations

Ausgewählte Quellen

- EU-Marineoperation ATALANTA, „Operation ATALANTA koordiniert multinationale Reaktion auf Piratenangriff auf MV GOLDEN ARSENAL", 3. Juli 2026.
- UKMTO, Seite „Recent Incidents", geprüft am 6. Juli 2026.
- ReliefWeb / OCHA, „Erdbeben in Venezuela: Lagebericht Nr. 11", 4.–5. Juli 2026.
- Institute for the Study of War, „Russian Offensive Campaign Assessment", 5. Juli 2026.
- International Institute for Strategic Studies, Drohnensichtungs-Analyse, veröffentlicht 2. Juli 2026.
- Ukrainische Behörden über Agenturberichte, Opferzahlen zu den Angriffen auf Kyjiw, 2. Juli 2026.
- Security Council Report, Monatsvorausschauen zu Westafrika/Sahel und Sudan, Juli 2026.
- UNICEF, Berichterstattung zu Kinderopfern im Sudan, zitiert Anfang Juli 2026.
- ACLED, „Middle East Overview: June 2026".
- AEI, „China & Taiwan Update", 26. Juni und 2. Juli 2026.
- KrebsOnSecurity, „FBI Seizes NetNut Proxy Platform, Popa Botnet", 2. Juli 2026.
- BleepingComputer, „NetNut proxy network disrupted, 2 million infected devices cut off", 3. Juli 2026.
- The Hacker News, „North Korean Hackers Publish 108 Malicious Packages and Extensions in PolinRider Campaign", 4. Juli 2026.
- InSight-Crime-Beiträge, 2.–3. Juli 2026, u. a. zu Ardillos, Chiquito Malo, Larry Changa und kriminellen Druckpunkten in Mexiko.
- Reuters/Agenturberichte, Ergebnis der Präsidentschaftsstichwahl in Kolumbien, Ende Juni/Anfang Juli 2026.
- Agentur- und Reisesicherheitsberichte, Sicherheitsaufgebot Mexikos zur FIFA-Weltmeisterschaft, Juni/Juli 2026.

Methodenhinweis

Dieser Bericht basiert auf öffentlich zugänglichem Quellenmaterial, das bis zum 6. Juli 2026 ausgewertet wurde, sowie auf der analytischen Einschätzung von SF Custos Global. Er ersetzt keine rechtliche, versicherungs-, sanktions-, medizinische oder länderspezifische Fachberatung.