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

WEEKLY SECURITY BRIEFING
29 Jun–5 Jul 2026

WEEKLY SECURITY BRIEFING · KW27 2026

Weekly Security Briefing

Author: Benjamin Traunecker

Executive Summary — This Week's Key Global Developments

Venezuela is facing its worst natural-disaster emergency in years. ReliefWeb and OCHA reported that two earthquakes of magnitude 7.2 and 7.5 struck the north-central region on 24 June, and by 4 July authorities had confirmed 2,954 deaths, 16,592 injuries, 6,462 rescues and more than 940 aftershocks, with La Guaira the worst-affected state. The scale sits above most single-country disasters SF Custos Global has tracked this year, and the security consequence is not the earthquake itself but the strain it puts on transport routes, medical capacity, local policing and aid distribution over the following weeks.

Russia ran a dual-track campaign against Ukraine this week: an information push around Kostyantynivka and a lethal strike campaign against Kyiv. The Institute for the Study of War assessed that the Kremlin was amplifying claims of having seized Kostyantynivka while Russian forces had in fact infiltrated but not consolidated control of the city, timed around President Trump's 4 July calls with Vladimir Putin and Volodymyr Zelensky. Separately, Russian missile and drone strikes on Kyiv on the night of 1–2 July killed at least 17 people and wounded more than 90, with damage recorded at more than 30 locations. Together, the two threads show Russia pairing narrative pressure with continued willingness to strike the capital directly.

Sudan's war has a new flashpoint. Fighting intensified around El Obeid, the capital of North Kordofan state, where the Sudanese Armed Forces have built roughly 51 kilometres of defensive berms and trenches and at least 14 checkpoints while the Rapid Support Forces encircle the city from the west, north and south. A senior UN official warned the window to prevent a major escalation is "rapidly narrowing," and UNICEF separately reported that more than 300 children have been killed or injured in the wider war over the past six months.

Piracy has returned as a confirmed, active threat in the Gulf of Aden. EUNAVFOR Operation ATALANTA reported that MV GOLDEN ARSENAL was attacked by armed men with assault rifles and RPGs approximately 110 nautical miles northeast of Bosaso, Somalia, on 1 July; a coordinated naval response secured the vessel with no injuries. ATALANTA assessed that a Pirate Action Group is likely active in or near the Internationally Recommended Transit Corridor, alongside three other ongoing piracy cases in the Somali Basin — a meaningful shift for any organisation that had deprioritised piracy risk in favour of the Houthi threat picture.

North Korea-linked actors escalated software supply-chain targeting. The Hacker News, citing Socket research, reported that operators connected to the Contagious Interview ecosystem published 108 malicious packages and browser extensions across npm, Packagist, Go and Chrome under the "PolinRider" activity set, aimed at developers and cryptocurrency-linked personnel through fake recruitment, poisoned repositories and malicious IDE tasks.

A parallel cybercriminal infrastructure network was dismantled. KrebsOnSecurity and BleepingComputer reported that the FBI, Google and industry partners seized domains tied to NetNut, a residential proxy service linked to the "Popa" botnet and, according to Google Threat Intelligence Group estimates, at least two million compromised consumer devices used to mask criminal and espionage traffic.

Colombia's presidential race concluded with a clear security-policy pivot. Abelardo de la Espriella won the run-off with 49.6% of the vote against Iván Cepeda's 48.7%, campaigning on expanded military deployments and closer coordination with

private security providers against the outgoing government's "total peace" negotiation approach — a result organisations with Colombian exposure should read as a likely shift in enforcement posture over the coming months.

Europe's hybrid-threat picture came into sharper focus. The International Institute for Strategic Studies published a tally of 144 suspected drone sightings linked to Russian "shadow fleet" vessels disrupting European civil aviation between 2024 and 2026, describing the campaign as deliberately calibrated to stay below the threshold that would trigger a collective NATO response — a pattern IISS called a demonstration that European air defences are not yet fit for the current threat environment.

Key Developments & Intelligence Assessment

Europe HIGH

Russia's public line on Kostyantynivka is a useful indicator of how Moscow intends to frame the next phase of diplomacy. ISW assessed on 5 July that Kremlin officials were presenting an alleged Russian seizure of the city to Western audiences, including around President Trump's 4 July calls with Putin and Zelensky. ISW also assessed that Russian forces had infiltrated parts of Kostyantynivka but had not seized it, and that Ukrainian forces retained a presence in parts of the city. Short ceasefire proposals around contested urban areas should be read carefully going forward: they may be humanitarian in form, but they can also serve battlefield positioning and negotiation-narrative pressure.

> Intelligence Assessment
> Medium Russia is likely to continue pairing battlefield pressure with claims designed for Western political consumption while sustaining direct strikes on Ukrainian population centres. The risk for companies is indirect but real: sanctions debates, reconstruction planning, insurance exposure, logistics routing and energy assumptions can all be affected by perceptions of battlefield momentum.

Russia's rear-area protection problem is becoming more visible. ISW reported that Gazprom had signed an arrangement with the Russian Ministry of Defense to create mobile fire groups for gas infrastructure, while Russian volunteer and military formations were also discussed in relation to drone defence — a sign that Ukrainian long-range strikes are forcing Russia to allocate manpower and attention away from other requirements.

> Intelligence Assessment
> Medium Ukrainian strike pressure on Russian energy and logistics sites is likely to remain a recurring business-risk driver. The immediate corporate effect is not battlefield movement; it is volatility in energy infrastructure, port and rail resilience, sanctions enforcement, insurance wording and supplier continuity.

ALSO MONITORED THIS WEEK

- **Kyiv strikes:** Russian missile and drone strikes on Kyiv overnight on 1–2 July killed at least 17 people and wounded more than 90, with damage recorded at more than 30 locations including 20 residential buildings and a medical facility, according to Ukrainian authorities.
- **Shadow-fleet drone campaign:** The International Institute for Strategic Studies published a report plotting 144 suspected drone sightings across Europe between 2024 and 2026, assessing that Russia likely used shadow-fleet vessels to launch drones that repeatedly disrupted civilian aviation while staying below the threshold for a collective NATO response.

- **Fehmarn Belt incident:** A Russian warship, reported as the "Savvy," was involved in an incident in the Fehmarn Belt Strait off the German coast on 30 June; separately, Montenegro is preparing to introduce visa requirements for Russian nationals, a signal of tightening regional posture toward Moscow.

Middle East ELEVATED

The strongest confirmed maritime development this week came from EUNAVFOR Operation ATALANTA. ATALANTA reported that MV GOLDEN ARSENAL was attacked on 1 July by armed persons with assault rifles and RPGs approximately 110 nautical miles northeast of Bosaso, Somalia. The crew implemented Best Management Practices, stopped the vessel, activated a distress alert and mustered in the citadel. ATALANTA coordinated with Combined Maritime Forces, the Republic of Korea Navy, the Indian Navy, IFC-IOR and regional authorities; Indian Navy warship INS TRIKAND deployed a helicopter and boarding team that secured the vessel with no injuries reported.

ATALANTA's current-piracy assessment matters more than the single incident: it stated that a Pirate Action Group is likely in the Internationally Recommended Transit Corridor and referenced three ongoing piracy cases in the Somali Basin involving HONOUR 25, EUREKA and SWARD. This places piracy back into the route-planning picture after years in which many operators treated it as secondary to Houthi-related missile and drone threats.

> Intelligence Assessment
> High The Gulf of Aden and Somali Basin now require a dual-risk reading: piracy and conflict-linked maritime threats can overlap in the same operating corridor. For commercial operators, the practical issue is not whether the next incident is labelled piracy or regional escalation; it is whether vessel profile, routing, crew procedures and naval-response access reduce exposure.

UKMTO's public recent-incidents page showed no reports at the time of verification. Several social media items referenced possible Red Sea or Gulf of Aden incidents, but those claims were not used as confirmed facts in this briefing because they could not be matched to the official UKMTO page during this run.

ALSO MONITORED THIS WEEK

- **Israel-Hezbollah ground expansion:** ACLED's June regional overview recorded a roughly 10% month-on-month rise in Israeli-Hezbollah attacks in May, with Israeli forces pushing north of the Litani River into al-Nabatieh district and expanding ground presence around the Beaufort Ridge and Wadi Saluki — a slower-burning escalation that received far less coverage than the Gaza and Iran tracks.
- **Yemen's internal rift:** The Houthis have largely stopped attacking Red Sea shipping since the Gaza ceasefire, but a new rift has opened between Saudi Arabia and the United Arab Emirates over the possible repartition of Yemen and over leadership of southern forces that have seized Yemeni oil fields — a dispute with direct implications for energy-sector access in southern Yemen.
- **Hormuz implementation friction:** Disputes over implementing the US-Iran memorandum of understanding continued to play out most visibly around the Strait of Hormuz, with the framework understood to only temporarily pause hostilities and reopen the strait while deferring Iran's nuclear programme and long-term sanctions relief.

Africa HIGH

The GOLDEN ARSENAL case confirms that the Horn of Africa maritime threat is active. The incident also shows that crew discipline and naval coordination can still prevent a successful hijack when reporting is timely and BMP-MS actions are followed — a reminder that the response chain still works when it is activated early, not a reason to downgrade risk.

> Intelligence Assessment
> High Somali piracy risk is no longer a low-priority background issue for vessels near the IRTC and Somali Basin. The current pattern is still containable, but only if vessels assume that armed groups can operate with enough reach to force citadel procedures and naval response.

Open-source social media streams reported fighting around Anéfis in Mali and possible losses involving Malian and Russian-aligned forces. The material was specific enough to warrant monitoring, but it was not independently confirmed by publication time through official, wire, NGO or established analytical channels available during this run and should stay below the threshold for a firm client-facing factual statement.

> Intelligence Assessment
> Low The Sahel remains structurally high risk, but the current-week Anéfis reporting should be treated as an indicator, not a confirmed event set. The watch item is whether JNIM, FLA-linked or other armed actors sustain pressure on military movement corridors in northern and central Mali.

ALSO MONITORED THIS WEEK

- **Sudan — El Obeid siege:** Fighting intensified around El Obeid, North Kordofan's capital, where the Sudanese Armed Forces have fortified the city with roughly 51 kilometres of berms and trenches and at least 14 checkpoints while the Rapid Support Forces encircle it from three directions; a senior UN official warned the window to prevent a major escalation is narrowing, and UNICEF reported more than 300 children killed or injured in the war over the past six months.
- **Nigeria — school abduction:** Gunmen raided Lassa Day Secondary School in Borno state's Askira-Uba area, abducting 25 girls, 11 boys and three teachers, amid intensified Nigerian military operations against Boko Haram and Islamic State West Africa Province in the Lake Chad Basin.
- **DR Congo — resource leakage:** A new UN report found that gold smuggling from DR Congo's Ituri province to Uganda is rising, with the gap between Uganda's declared gold exports and its own production increasingly explained by smuggled Congolese material — a slower-moving governance risk with direct relevance for supply-chain and sanctions-exposure due diligence.

Asia ELEVATED

The Hacker News, citing Socket research, reported that North Korea-linked actors connected to the Contagious Interview campaign published 108 unique packages and browser extensions across npm, Packagist, Go and Google Chrome as part of PolinRider. The activity reportedly includes 162 malicious release artefacts, malicious JavaScript loaders, developer social engineering, compromised maintainer paths and execution through developer tooling such as VS Code task files.

The targeting logic is clear. Developers, crypto workers and maintainers are attractive because their machines bridge personal trust, code repositories and production environments. A poisoned package does not need to breach a firewall first if it can persuade a developer to install, test or open the wrong project.

> Intelligence Assessment
> Medium North Korea-linked software supply chain activity is likely to remain a recurring corporate risk because it exploits hiring, freelancing and developer trust rather than only perimeter weakness. The most exposed organisations are those with fast-moving engineering teams, weak package governance or cryptocurrency-related access.

ALSO MONITORED THIS WEEK

- **Taiwan Strait — quieter month:** Taiwan's defence ministry recorded 12 days in June without any People's Liberation Army incursions across the Taiwan Strait median line, a reversion toward the pre-2024 baseline after PLA activity had roughly doubled following President Lai's 2024 inauguration — a de-escalation signal worth tracking rather than assuming as a trend.
- **Scarborough Shoal presence-building:** A PRC coastal research vessel, Tong Ji, sailed to Scarborough Shoal shortly after a platform there was removed, consistent with an assessed pattern of Beijing building a more permanent or semi-permanent manned presence to reinforce its territorial claim.
- **Carrier rotations:** PLAN aircraft carrier Liaoning returned to its home port of Qingdao on 23 June after an over 40-day deployment in the South China Sea and West Pacific, while carrier Fujian continued transits through the Taiwan Strait — activity consistent with more frequent PLA carrier rotation between theatre commands.

Latin America / Caribbean HIGH

ReliefWeb / OCHA reported that Venezuela was facing a national emergency after two earthquakes of magnitude 7.2 and 7.5 struck the north-central region on 24 June. By 4 July, authorities reported 2,954 deaths, 16,592 injured people, 6,462 rescues, more than 940 aftershocks and approximately 16,309 people who had lost their homes, with La Guaira the most affected state. The UN system and partner organisations were responding with multisectoral support in coordination with the government.

> Intelligence Assessment
> High Venezuela's earthquake emergency is a major humanitarian and operating-environment shock. The next risk phase will be shaped by aftershocks, shelter capacity, medical strain, road access and the state's ability to manage aid distribution without worsening local security conditions.

InSight Crime's feed this week carried analysis and profiles connected to Mexico's Ardillos, Colombia's Chiquito Malo and Venezuela's Larry Changa, alongside a piece on Mexico's criminal pressure points: drugs, corruption and CJNG fuel theft. Haiti remains a severe security concern; social media and specialist commentary again pointed to gang control and restricted mobility in Port-au-Prince, though the specific figures circulating were not independently verified by publication time.

> Intelligence Assessment
> Medium Organised-crime pressure in Latin America is not a single-country problem. The common mechanism is criminal control over infrastructure, prison systems, fuel flows, ports, neighbourhood access and local political protection. For companies, the exposure shows up as route disruption, extortion risk, unreliable local contractors and sudden changes in law-enforcement posture.

ALSO MONITORED THIS WEEK

- **Colombia's election result:** Abelardo de la Espriella won Colombia's presidential run-off with 49.6% of the vote against Iván Cepeda's 48.7%, campaigning on expanded military deployment and closer coordination with private security companies against the outgoing "total peace" approach — a result likely to shift enforcement posture toward armed groups over the coming months.

- **Mexico World Cup security posture:** Mexico has deployed close to 100,000 military and federal police personnel across host cities for the 2026 FIFA World Cup, which runs from 11 June to 19 July and is expected to draw approximately 5.5 million international visitors — a concentrated security operation with direct relevance for any organisation moving personnel through host cities during the tournament window.
- **Ecuador-Colombia friction:** Cross-border tension between Colombia and Ecuador, including an earlier trade dispute between the two governments, continues to complicate calls for deeper security cooperation on shared border areas used by organised-crime networks.

Global Cyber / Critical Infrastructure HIGH

KrebsOnSecurity reported on 2 July that the FBI worked with industry partners to seize hundreds of domains associated with NetNut, a residential proxy service linked by security firms to the Popa botnet. Krebs cited Google Threat Intelligence Group reporting that NetNut was widely resold and used by cybercriminal and espionage groups to mask source IP addresses, access victim environments and conduct password-spraying attacks. BleepingComputer reported that Google estimated the network included at least two million compromised devices, including smart TVs and streaming boxes, and that Google, the FBI, Lumen, Shadowserver and other partners were involved in the disruption.

> Intelligence Assessment
> High The NetNut / Popa disruption will probably reduce some criminal capacity in the short term, but the proxy ecosystem is resilient. Operators can buy replacement capacity, resell access and shift to other providers. Security teams should expect degradation, not disappearance, of residential-proxy-enabled abuse.

The North Korea-linked PolinRider reporting intersects with this picture. Malicious packages, browser extensions, IDE tasks and repository-history manipulation make the developer environment a target environment, especially for companies that rely on third-party code dependencies, rapid CI/CD processes or contractors with broad repository access.

> Intelligence Assessment
> Medium Software supply chain attacks remain attractive because they convert trust into access. The next useful indicators are malicious package clusters, unusual maintainer account behaviour, hidden IDE execution tasks and post-install scripts that reach external infrastructure.

Global Intelligence Assessment

The week did not produce one single global shock that overrides all other risks. It produced a clearer picture of how several risk systems now overlap. Russia is trying to turn battlefield narratives into diplomatic pressure while continuing to strike Ukrainian cities directly, and its shadow-fleet drone campaign shows the same calibrated-pressure logic applied to European airspace. Maritime operators in the Gulf of Aden must account for piracy again while still watching the Red Sea conflict environment and the slower Israel-Hezbollah escalation north of the Litani River. Cyber actors are using residential devices, package repositories and developer trust as infrastructure, largely independent of any single geopolitical flashpoint. Sudan's war and Venezuela's earthquake show two very different routes to the same outcome: state capacity that cannot keep pace with the scale of the crisis. Latin America adds a third layer — organised crime, an election that will likely harden enforcement posture, and a major sporting event drawing a historic security deployment, all inside the same reporting week.

For companies, the practical issue is compression. Security decisions increasingly have to account for multiple risk mechanisms at the same time: a vessel can face piracy and conflict exposure in one corridor; a developer laptop can become a route into production; a natural disaster can become a mobility, shelter and public-order issue; a battlefield claim can influence sanctions, insurance and political assumptions before the facts are stable; an election result can change enforcement posture faster than any single incident.

The strongest confirmed signals this week are OCHA's Venezuela earthquake data, EUNAVFOR's report on MV GOLDEN ARSENAL, UN reporting on the El Obeid siege, KrebsOnSecurity and BleepingComputer reporting on NetNut / Popa, The Hacker News reporting on North Korea-linked malicious packages, and Colombia's certified election result. The weakest signals are current-week social media claims on Mali and uncorroborated Red Sea incident reports. They remain useful watch items but should not drive decisions without further corroboration.

Near-term watch indicators: additional ATALANTA or UKMTO maritime alerts near the IRTC; evidence of further Pirate Action Group activity; whether El Obeid's defensive lines hold or are breached; Ukrainian long-range strikes against Russian energy or logistics sites and any further Russian strikes on Kyiv; malicious package clusters tied to developer tooling; and confirmed humanitarian access changes in Venezuela.

Watch Indicators

- **Kostyantynivka and ceasefire signalling:** any formal ceasefire or humanitarian-corridor proposal tied to the city, and whether it coincides with continued Russian strikes elsewhere in Ukraine.
- **Somali Basin piracy tempo:** additional ATALANTA, UKMTO or EUNAVFOR reporting on incidents or Pirate Action Group sightings near the Internationally Recommended Transit Corridor within the next two to three weeks.
- **El Obeid's defensive perimeter:** satellite or wire confirmation of whether the Sudanese Armed Forces' berm-and-checkpoint line holds, is breached, or is abandoned, and any UN statement escalating from warning language to confirmed atrocity reporting.
- **Developer-tooling compromise clusters:** new npm/Packagist/Go/Chrome package takedowns or advisories referencing PolinRider infrastructure, IDE task-file abuse or Contagious Interview recruitment lures.
- **Venezuela aftershock and access data:** OCHA situation report updates showing whether death/injury figures are stabilising and whether road, port and airport access is being restored or is deteriorating further.
- **Colombia security-policy transition:** concrete announcements from the incoming de la Espriella government on military deployment levels, private-security coordination or the status of the outgoing "total peace" negotiations with armed groups.
- **Fehmarn Belt and Baltic maritime incidents:** further reporting on Russian naval activity in the Baltic approaches, and whether other states follow Montenegro's move toward tighter Russian visa restrictions.

Glossary of Abbreviations

Abbreviation	Meaning
ATALANTA	European Union Naval Force Operation 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	Internationally Recommended Transit Corridor

Abbreviation	Meaning
ISW	Institute for the Study of War
JNIM	Jama'at Nusrat al-Islam wal-Muslimin
OCHA	United Nations Office for the Coordination of Humanitarian Affairs
PAG	Pirate Action Group
PLA / PLAN	People's Liberation Army / People's Liberation Army Navy
RSF	Rapid Support Forces (Sudan)
SAF	Sudanese Armed Forces
UKMTO	United Kingdom Maritime Trade Operations

Selected Sources

- EUNAVFOR Operation ATALANTA, "Operation ATALANTA coordinates multinational response to pirate attack on MV GOLDEN ARSENAL," 3 July 2026.
- UKMTO, Recent Incidents page, checked 6 July 2026.
- ReliefWeb / OCHA, "Earthquakes in Venezuela: Situation Report No. 11," 4–5 July 2026.
- Institute for the Study of War, "Russian Offensive Campaign Assessment," 5 July 2026.
- International Institute for Strategic Studies, drone-sightings analysis reported 2 July 2026.
- Ukrainian authorities via wire reporting, Kyiv strike casualty figures, 2 July 2026.
- Security Council Report, "West Africa and the Sahel" and Sudan-related July 2026 monthly forecasts.
- UNICEF, Sudan child casualty reporting, cited early July 2026.
- ACLED, "Middle East Overview: June 2026."
- AEI, "China & Taiwan Update," 26 June and 2 July 2026.
- KrebsOnSecurity, "FBI Seizes NetNut Proxy Platform, Popa Botnet," 2 July 2026.
- BleepingComputer, "NetNut proxy network disrupted, 2 million infected devices cut off," 3 July 2026.
- The Hacker News, "North Korean Hackers Publish 108 Malicious Packages and Extensions in PolinRider Campaign," 4 July 2026.
- InSight Crime RSS items, 2–3 July 2026, including Ardillos, Chiquito Malo, Larry Changa and Mexico criminal pressure point items.
- Reuters/wire reporting, Colombia presidential run-off result, late June–early July 2026.
- Wire and travel-security reporting, Mexico FIFA World Cup security deployment, June–July 2026.

Method Note

This report is based on open-source material reviewed up to 6 July 2026 and analytical assessment by SF Custos Global. It does not replace legal, insurance, sanctions, medical or country-specific professional advice.