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

WEEKLY SECURITY BRIEFING
3–10 Aug 2026

WEEKLY SECURITY BRIEFING · KW33 / 2026

Weekly Security Briefing

Author: Benjamin Traunecker

Executive Summary — This Week's Key Global Developments

1. **Ukraine moved its rear-area strike campaign from episodic pressure to a measurable Russian business problem.** The Institute for the Study of War reported on 4 August that Ukraine's Security Service said it had conducted more than 100 successful strikes in the first 40 days of a wide campaign against Russian military, logistics, industrial and energy targets. Reuters reporting during the week separately tracked fires and damage at Russian refinery sites, including Ilsky and Yaroslavl, while later Reuters summary reporting described a broader acceleration against Russian energy infrastructure. The operational signal is that Ukraine is no longer treating long-range strikes only as battlefield support; it is using them to stress Russian fuel, insurance, repair, air-defence and public-confidence systems.

2. **The Red Sea returned to an acute maritime-risk track before the later cargo-ship casualty event.** Al Jazeera, citing AFP, Reuters and AP, reported on 10 August that Houthi missile and drone attacks on Yemen's Red Sea port city of al-Makha killed seven more people and wounded around 30 after an earlier strike wave killed at least 11. The attacks hit government-held coastal areas, port infrastructure, electricity generation and civilian facilities, while government-aligned forces said air defences intercepted drones and an explosive boat. For shipping, port operations and evacuation planning, the point is clear: western Yemen moved into a higher-tempo strike cycle before the subsequent vessel attack off al-Makha.

3. **Mali's San base attack showed that central Mali remains within JNIM's operational reach.** AFP reporting carried by Seneweb said at least 10 Malian soldiers were killed on 9 August when JNIM attacked an army camp in San, in Ségou region. A security source said the camp was temporarily occupied before the army regained control; the Malian general staff framed it as an attempted attack repelled by a vigorous response. The gap between official, local and militant narratives is itself operationally relevant: organisations moving through central Mali should assume verification lags, road conditions can shift quickly, and base security does not automatically translate into corridor security.

4. **Northwestern Nigeria remained capable of producing high-casualty security-force engagements despite rescue operations elsewhere.** Al Jazeera and AFP reported on 11 August that at least 10 police officers, 17 armed men and two civilians were killed after police confronted an armed group of roughly 240 men on more than 200 motorcycles in Kebbi State. The clash occurred on 10 August as the group moved from Zamfara toward Kebbi. The incident is a useful warning against reading single rescue announcements as durable stabilisation: armed groups in the northwest retain mobility, manpower and tactical mass.

5. **Asia's main signal was exercise escalation rather than immediate crisis.** Associated Press reporting carried by the Boston Herald on 10 August said South Korea and the United States would begin the annual Ulchi Freedom Shield exercise on 17 August for an 11-day run, involving about 18,000 South Korean soldiers and incorporating lessons from recent conflicts. The announcement came days after North Korea resumed ballistic missile testing, which South Korea, Japan and the United States condemned. The immediate business risk is not war; it is the shortening of warning time around airspace, maritime, diplomatic and cyber signalling whenever exercises and missile activity overlap.

6. **Colombia's new government signalled a harder security partnership with Washington.** The U.S. State Department said on 7 August that Washington, working with Congress, intended to announce $1 billion in assistance as part of a security package for President Abelardo de la Espriella's administration. Reuters reported the same plan and framed it around the new right-wing government's security orientation. The package is stated intent rather than disbursed money, but it matters because security-force support, coca-eradication pressure and counter-narcotics operations can change movement and retaliation risk before outcomes are visible.

7. **Mexico and Haiti kept Latin America and the Caribbean on the operating-risk map.** El País reported on 10 August that cartel violence had spread toward Mazatlán, with up to 32 violent events officially recorded in the first week of August, 14 murders and drone attacks that injured state police officers on the Mazatlán-Culiacán bypass. UN Security Council reporting on Haiti in July, supplemented by August local reporting, kept gang violence, elections, displacement and security-force capacity at the centre of the Caribbean risk picture. Both cases show why city, route and neighbourhood exposure matters more than national labels.

8. **Cyber exposure remained tied to ordinary business infrastructure.** CISA, FBI and partner agencies released advisory AA26-222A on Gunra ransomware on 10 August, according to official advisory tracking used for this retrospective issue. The advisory describes a ransomware-as-a-service pattern with double extortion and initial access through known vulnerabilities in internet-facing systems. For security managers, this makes cyber a weekly operating issue, not a separate technical appendix: exposed VPNs, edge appliances, backup posture and incident-response readiness can compound physical crisis exposure.

Key Developments & Intelligence Assessment

Europe HIGH

Ukraine expands pressure against Russian energy and logistics

Ukraine's long-range campaign is now stressing the Russian rear rather than merely demonstrating reach. ISW assessed on 4 August that Ukraine's Security Service announced more than 100 successful strikes in the initial 40 days of a campaign that began on 26 June. The target set included defence-industrial enterprises, air bases, air-defence assets, command posts, warships, tankers, oil refineries, transport nodes and military logistics. ISW also reported Ukrainian claims of strikes against 14 oil refineries and other oil infrastructure objects, two cargo ships and two shadow-fleet oil tankers. This is not a single spectacular attack; it is a systematic attempt to raise the cost of Russia's war across multiple rear-area systems at the same time.

The commercial impact sits in fuel, insurance and air defence allocation. ISW cited Bloomberg and Russian business reporting indicating that refinery pressure forced Russia to export near-record crude volumes while domestic refining rates fell sharply, and that Russian insurance companies had effectively stopped covering certain military and terrorist risks for cargo ships operating in Black and Azov Sea waters. Reuters reporting during the week tracked Ukrainian drone-linked incidents at Russian refinery sites, including Ilsky and Yaroslavl. Exact damage estimates vary by facility and are often slow to verify, but the pattern is clear enough: Ukraine is forcing Russia to defend and repair critical infrastructure far from the front line while sustaining pressure on maritime and energy-linked business assumptions.

> Intelligence Assessment
> High Europe remains high risk. Confidence is high that Ukraine's rear-area strike campaign widened during the reporting week and that Russian energy, maritime-insurance and logistics systems are under cumulative pressure. Confidence is lower for individual damage figures at specific refinery sites because Russian, Ukrainian and commercial reporting often diverge. The client-relevant judgment is that the war is creating more business exposure through logistics, insurance, repair capacity and retaliatory-strike risk, not less.

Russian counter-pressure continued against Ukrainian infrastructure. ISW's 4 August assessment also described Russian long-range drone and missile activity against Ukraine overnight, while Ukrainian officials continued to press partners for interceptors and air-defence support. The combined picture matters for European organisations because escalation can appear through power disruption, rail and port delays, changed cargo terms, or sudden government movement restrictions. A strike inside Russia can still translate into risk for operations in Ukraine if Moscow retaliates against ports, utilities or civilian infrastructure.

Belarus and the Black Sea remained secondary watch areas. ISW's weekly reporting kept Belarus and Crimea-linked infrastructure under watch, while strike and insurance signals in the Black and Azov seas reinforced the broader maritime-risk environment. These areas did not displace the refinery campaign as the week's lead, but they are part of the same corridor-risk picture. Organisations exposed to sanctions, dual-use goods, ship management or agricultural flows should treat the week as a continuation of a wider war-economy contest.

ALSO MONITORED THIS WEEK

- **Russian refinery incidents remained cumulative.** Reuters and regional reporting on Ilsky, Yaroslavl and other energy sites should be read as part of a sequence, not as isolated facility events.
- **Insurance language is a live operational indicator.** Any further withdrawal, narrowing or repricing of war-risk cover in Black Sea, Azov Sea or Russian-linked cargo trades should be treated as an early warning of real operating friction.

- **Air-defence allocation matters for both sides.** Russia must protect more rear-area nodes, while Ukraine remains dependent on interceptors against Russian mixed strike packages.

Middle East HIGH

Yemen's western coast moved into a higher-tempo strike cycle

Al-Makha became the week's clearest Middle East warning signal. Al Jazeera reported on 10 August, citing AFP, Reuters and AP, that Yemen's Houthis launched a new wave of missile and drone attacks on the Red Sea port city of al-Makha, killing seven more people and wounding around 30 after an earlier strike wave killed at least 11. Yemen's armed forces said the later attack killed four military personnel and three civilians, and that most of the wounded were civilians. The reported target set included civilian facilities, infrastructure, homes, electricity-generation stations and military positions. The attack came before the later cargo-vessel casualty incident, making it an important precursor rather than a footnote.

Port, coastal and maritime risk are now linked. The same reporting said earlier strikes caused extensive damage at al-Makha's port, including port infrastructure, commercial goods and food supplies, while government forces said they intercepted an unmanned explosive boat approaching the commercial port. Houthi statements framed the operation as a response to Saudi military buildup and targeted military concentrations and weapons depots. For a client-facing assessment, the safest formulation is not to accept either side's full narrative. The confirmed issue is that a government-held Red Sea port and nearby coastal infrastructure were hit by a combined missile, drone and explosive-boat threat environment.

> Intelligence Assessment
> High Middle East maritime and coastal risk is high. Confidence is high for the al-Makha attack sequence, the casualty reporting and the port-infrastructure relevance because multiple recognised outlets cited AFP, Reuters, AP and Yemeni military accounts. Confidence is medium for precise targeting intent because Houthi and government narratives diverge. The operational assessment is firm: western Yemen remains capable of producing multi-vector attacks that affect port operations, vessel routing, coastal movement and evacuation planning.

The Red Sea signal reaches beyond Yemen. A missile and drone cycle against al-Makha does not automatically mean every commercial vessel in the Red Sea faces the same probability of attack, but it changes the risk conversation for crews, insurers and route planners. Strike tempo on shore can precede or accompany attacks at sea. Any vessel linked to Saudi, coalition, Israeli, U.S., UK or perceived hostile interests may face higher scrutiny, and even unrelated shipping can be affected by rerouting, naval warnings, rescue constraints or sudden port closures.

Iran and Gulf escalation remained a linked watch area. The reporting reviewed for W33 did not support a stronger fresh Hormuz incident than the al-Makha lead within the strict 3–10 August window. However, Yemen's Red Sea escalation and regional military positioning keep the broader Gulf risk architecture sensitive. The key operating issue is less whether a single incident proves a regional plan and more whether multiple corridor pressures begin affecting the same shipping, insurance and emergency-response systems.

ALSO MONITORED THIS WEEK

- **Explosive-boat claims matter.** Even an intercepted unmanned boat near a commercial port is a warning for harbour security, stand-off distances and small-craft monitoring.
- **Civilian infrastructure was within the strike envelope.** The reported damage to electricity generation, homes and commercial goods means coastal movement and aid logistics should not be treated as protected by default.
- **Maritime advisories require daily review.** UKMTO, IMO, JMIC, EUNAVFOR and flag-state notices remain more useful for immediate movement decisions than political rhetoric alone.

Africa HIGH

Sahel and northwestern Nigeria showed armed-group tactical mass

The San attack demonstrated that JNIM can still challenge fixed positions in central Mali. AFP reporting carried by Seneweb said at least 10 Malian soldiers were killed on 9 August during an attack against a Malian army camp in San, in central Mali's Ségou region. A security source said the camp was temporarily occupied before the army regained control. The Malian general staff described the incident as an attempted attack on the FAMa base at about 5:30 a.m. and said a vigorous response repelled it. JNIM claimed total control of the barracks during the morning. The contradictory claims do not cancel each other; they show how quickly the information environment becomes contested during an attack.

For movement planning, the base is less important than the corridor. San sits in a region relevant to central Mali road movement and state-force reach. If militants can launch a dawn attack, force a temporary occupation claim and compel a public military response, organisations should assume the surrounding road network can degrade faster than official updates acknowledge. Escorts, fuel stops, local staff movements and contractor convoys need more than a simple "army base present" assumption. The same week also followed a July attack in which at least 50 soldiers were reportedly killed in northern Mali, reinforcing that the Malian security environment remains under heavy pressure.

> Intelligence Assessment
> High Africa risk is high for the Sahel and selected West African corridors. Confidence is high for the San attack, the JNIM claim and the reported Malian military response; confidence is medium for final control and exact losses beyond the AFP-cited minimum because state and militant narratives diverge. The practical assessment is that central Mali remains exposed to high-tempo militant operations that can disrupt movement, military response assumptions and local partner reliability.

Northwestern Nigeria showed a separate but related pattern of tactical mass. Al Jazeera and AFP reported on 11 August that police confronted a heavily armed group of about 240 men on more than 200 motorcycles in Kebbi State on 10 August. At least 10 police officers, 17 armed men and two civilians were killed, with two officers wounded. The group was reportedly moving from Zamfara toward Kebbi. The size of the group and the motorcycle mobility are more important than the final casualty number: armed actors can cross state boundaries, mass quickly and overwhelm or fix security units even when authorities conduct successful rescue or interdiction operations elsewhere.

Nigeria's rescue narrative should not be mistaken for stabilisation. Earlier in August, Nigerian authorities announced the rescue of 308 abducted people in Niger and Kwara states, which was a meaningful tactical success. The Kebbi clash shows the other side of the operating picture. Rescue success and armed-group mobility can coexist. For companies, NGOs and diplomatic travel, that means route risk remains time-sensitive and local. A state-level security improvement may not protect a convoy, district office, school route or contractor movement if armed groups are already mobile nearby.

ALSO MONITORED THIS WEEK

- **Mali's junta legitimacy remains tied to security delivery.** A claimed militant penetration of a military camp undermines the narrative that Russian-aligned security partnerships have restored state control.
- **Motorcycle columns remain an early-warning indicator in Nigeria.** Reports of large armed motorcycle movements should be treated as more than routine banditry; they can precede high-casualty engagements.
- **Somalia, Sudan and eastern DR Congo remained structurally severe.** They did not produce a cleaner W33 lead than Mali or Kebbi in this run, but they remain high-priority monitoring areas for future weeklies.

Asia ELEVATED

Exercise planning and missile activity tightened the Korean Peninsula watch picture

Ulchi Freedom Shield moved from schedule item to regional signal. Associated Press reporting carried by the Boston Herald on 10 August said South Korea and the United States announced that their annual Ulchi Freedom Shield exercise would begin on 17 August and run for 11 days. South Korean officials said the scale would be similar to previous years, with about 18,000 South Korean soldiers participating. U.S. officials said the exercise would incorporate realistic threats and lessons from recent conflicts, including North Korean troops' reported battlefield experience in Ukraine. That changes the exercise from routine readiness into a signal about how the alliance is adapting to North Korea's evolving capability set.

North Korea's missile activity increased the messaging risk. The same AP report said South Korea, the United States and Japan detected a short-range ballistic missile launch from North Korea on the Thursday before the announcement. The missile landed in waters off North Korea's east coast, and the launch was condemned as a provocation or threat because UN Security Council resolutions prohibit North Korean ballistic activity. North Korea has historically framed major U.S.-South Korean exercises as invasion rehearsals. This creates a familiar but still consequential cycle: drills invite rhetoric, rhetoric can accompany tests, and tests can trigger allied demonstrations.

> Intelligence Assessment
> Medium Asia risk is elevated. Confidence is high for the exercise announcement, approximate participation figure and recent missile launch reporting. Confidence is medium for escalation forecasting because exercises and missile tests are partly signalling tools. The client relevance is strong: airspace, maritime, diplomatic, cyber and personnel-security risk can change during an exercise cycle even without a deliberate decision to escalate toward war.

Taiwan remained a parallel resilience watch area. The strongest Taiwan exercise detail in the available source set fell just outside the strict W33 cutoff, but the broader early-August picture kept civil resilience, anti-blockade planning and PRC jurisdiction signalling in focus. For a retrospective W33 product, Taiwan should therefore be treated as an "also monitored" item rather than the lead Asia development. The practical business issue remains continuity: ports, air routes, telecoms, semiconductor supply chains and executive travel can become exposed to administrative pressure or exercises even when no shots are fired.

Myanmar and South China Sea issues stayed below the lead threshold in this week. UN and regional reporting continued to show severe civilian exposure in Myanmar and contested maritime signalling in Asia, but the cleanest W33 development was the Korean exercise-and-missile cycle. That does not reduce structural risk. It only means the issue's lead focus should remain on the observable event with the best date fit and strongest sourcing.

ALSO MONITORED THIS WEEK

- **North Korean Ukraine lessons matter.** If North Korean forces bring battlefield lessons from Russia's war into doctrine, U.S.-ROK exercise design will continue to change.
- **Exercise periods are cyber-watch periods.** Korean Peninsula drills can coincide with phishing, disruption, GPS spoofing or influence activity even when physical escalation remains controlled.
- **Taiwan Strait administrative pressure remains relevant.** Shipping and aviation planners should monitor PRC traffic-control, coast guard and maritime-administration statements around the Strait.

Latin America / Caribbean ELEVATED

Security pivots and criminal violence remained the main operating-risk drivers

Colombia's new administration signalled an immediate hard-security alignment with Washington. The U.S. State Department said on 7 August that a U.S. presidential delegation attended President Abelardo de la Espriella's inauguration and that Washington, working with Congress, intended to announce $1 billion in assistance as part of a security package. The fact sheet said the package would support efforts to strengthen security forces, disrupt foreign terrorist organisations and transnational criminal organisations, expand coca eradication and cocaine interdiction, improve border security and reclaim territory once controlled by armed groups. Reuters reported the same plan and framed it around the new government's security orientation.

The announcement can change risk before the money arrives. The $1 billion figure is intent, not disbursed funding, and depends on Congress. Even so, armed groups, political opponents, local officials and security forces can respond to the signal immediately. Counter-narcotics pressure and efforts to reclaim territory can improve security over time if state capacity follows. They can also generate retaliation, road disruption, extortion pressure, protest or pressure on rural communities during the first operational phase. Companies with Colombia exposure should watch where operations begin, which groups are targeted, and whether cleared areas remain held after the initial deployment.

> Intelligence Assessment
> Medium Latin America and Caribbean risk is elevated. Confidence is high for the U.S.-Colombia policy signal and for reported violence in Sinaloa and Haiti. Confidence is medium for near-term operational effects because state security pivots can reduce some threats while provoking others. The business exposure sits around movement permissions, local partner reliability, port and road disruption, extortion pressure, hotel-zone security and emergency-response bandwidth.

Mazatlán became a sharper Mexico watch item. El País reported on 10 August that cartel violence had spread toward Mazatlán as the war in Sinaloa fragmented. The article said up to 32 violent events were officially recorded in the first week of August, with 14 people confirmed murdered and eight injured. Among the injured were three state police officers attacked by drones on the Mazatlán-Culiacán bypass near El Chilillo. The report also described more than 6,000 Army, National Guard, Navy and federal security personnel deployed around tourist zones. That combination is important: heavy state presence can protect priority districts while violence persists in worker neighbourhoods, bypasses and surrounding towns.

Haiti remained the Caribbean's most severe structural watch item. UN Security Council reporting in July described Haiti as caught between a return to order and a slide toward chaos, with gang violence exacting a heavy toll, millions displaced or food insecure and elections dependent on credible security conditions. August local reporting described renewed gang attacks and concern over election security. Even if a specific August incident cannot be verified to the same standard as the Colombia and Mexico leads, the operating reality remains severe: gangs influence transport routes, economic lifelines, police movement and civilian access, while the international Gang Suppression Force remains capacity-constrained.

ALSO MONITORED THIS WEEK

- **Colombia's territorial-control language is the key trigger.** Watch for operations aimed at "reclaiming, holding and building" state presence in former armed-group zones.
- **Mazatlán risk is micro-geographic.** Tourist districts, worker neighbourhoods, bypasses and mountain communities can face different levels of exposure on the same day.

- **Haiti's election calendar remains security-dependent.** Voter registration, campaign movement and polling logistics will be vulnerable if gang territorial control and police capacity do not improve.

Cyber / Critical Infrastructure ELEVATED

Gunra ransomware reinforced exposure in ordinary business systems

The official ransomware signal came at the end of the reporting week. CISA, FBI and partner agencies released cybersecurity advisory AA26-222A on Gunra ransomware on 10 August, according to official advisory tracking used for this retrospective issue. The advisory described a ransomware-as-a-service operation using double extortion and initial access through known vulnerabilities in internet-facing systems. Even where sector targeting is broad, the exposure pattern is familiar: edge devices, remote access, backups, segmentation and incident-response maturity determine whether an organisation absorbs or amplifies an intrusion.

The relevance is cross-domain. This Weekly treats cyber as part of the same operational environment as ports, logistics, executive travel and local partner networks. A ransomware event during a maritime rerouting, civil unrest episode, election period or armed-group attack can produce a compound crisis. Organisations with weak VPN controls, unmanaged remote access, untested backups or unclear escalation authority can lose situational awareness just when the physical environment is deteriorating.

> Intelligence Assessment
> Medium Cyber risk is elevated. Confidence is high that official U.S. cyber agencies treated Gunra as a current ransomware threat in the period. Confidence is medium for organisation-specific exposure without direct technical telemetry. The most useful assessment is that ordinary business infrastructure remains the probable entry point, making cyber hygiene a physical-security enabler rather than a separate IT concern.

ALSO MONITORED THIS WEEK

- **Remote access remains a priority control.** VPNs, edge appliances and exposed management interfaces should remain the first audit focus after any new ransomware advisory.
- **Backups need crisis-context testing.** A backup that works in normal conditions may fail if the same incident also affects logistics, telecoms or third-party providers.
- **Ransomware timing can be opportunistic.** Attackers do not need to understand a geopolitical crisis fully to exploit distraction, staffing gaps or delayed patch windows.

Global Intelligence Assessment

W33 was defined by pressure on corridors and state capacity. The most important developments did not sit inside one conflict. Ukraine pressed Russian energy and maritime systems; Yemen's western coast absorbed missile and drone attacks; Mali and Nigeria showed armed-group mass; Korea moved into an exercise-and-missile cycle; Colombia signalled a hard-security pivot; Mazatlán and Haiti showed the limits of state control in urban and route environments. The through-line is practical: routes, ports, bases, tourist zones, border areas and remote-access systems can become exposed before a national-level risk label changes.

State action did not automatically equal state control. Russia can still strike Ukraine while struggling to protect rear-area infrastructure. Mali can claim an attack was repelled while local sources report temporary occupation and soldier deaths. Nigeria can announce major rescues while armed groups still mass across state boundaries. Colombia can align with Washington before anyone knows whether new operations will hold territory. Mexico can deploy thousands of personnel around tourist zones while violence continues nearby. The operating lesson is that clients should monitor whether the state can sustain control after the first visible response.

Attribution discipline remains central. Several W33 developments invite easy overstatement. Houthi attacks are clear, but each claimed target should still be separated from confirmed impact. Mali's San attack is clear, but final control and casualty detail remain contested. Colombia's package is planned assistance, not completed funding. CISA's ransomware advisory identifies a threat pattern, not a breach at every exposed organisation. A good security product protects the reader from both underreaction and overclaiming.

The cyber-physical link was visible again. The same week contained port attacks, refinery disruption, armed-group mobility and ransomware warnings. This is the normal operating environment for clients: a crisis rarely stays in one domain. A port closure affects logistics platforms; a ransomware incident affects movement approvals; a refinery strike affects insurance and sanctions screening; gang violence affects hotel and transport choices. Security planning that separates cyber, travel, facilities and geopolitical analysis will miss the way these risks combine.

The practical watch stance is route-first and trigger-based. The next useful warning will often be a concrete movement or infrastructure signal: a maritime advisory, a refinery outage, a sudden checkpoint, a cancelled convoy, an embassy movement notice, a hotel-zone incident, a revised insurance clause, a cyber advisory naming an exploited vulnerability, or a government order changing exercise posture. Those signals should drive operational review faster than broad political commentary.

Watch Indicators

- Further Ukrainian strikes against Russian refineries, oil terminals, tankers, air bases, bridges or defence-industrial facilities, especially if accompanied by insurance or fuel-market disruption.
- Russian retaliatory strikes against Ukrainian ports, energy infrastructure, rail logistics or urban areas following deep Ukrainian attacks.
- New UKMTO, IMO, JMIC, EUNAVFOR or flag-state notices around Red Sea, Bab el-Mandeb, Gulf of Aden or al-Makha incidents involving missiles, drones, explosive boats, boardings or casualties.
- JNIM attempts to replicate the San attack pattern against additional bases, roads or towns in central and southern Mali.
- Reports of large armed motorcycle columns or cross-state armed-group movement in Nigeria's northwest.
- North Korean missile launches, GPS disruption, cyber activity or official threats before or during Ulchi Freedom Shield.
- Colombian announcements turning the planned U.S. security package into named operations, deployments, eradication campaigns or territorial-control efforts.
- New violent events affecting Mazatlán tourist districts, bypasses, hotel-worker neighbourhoods or highway access points.
- Haiti election milestones that require campaign movement, voter registration expansion or polling logistics in gang-influenced areas.
- CISA/FBI updates naming new exploited vulnerabilities, critical-infrastructure victims or active exploitation linked to Gunra ransomware.

Glossary of Abbreviations

Abbreviation	Meaning
AP	Associated Press
CISA	Cybersecurity and Infrastructure Security Agency
CNI	Critical national infrastructure
FBI	Federal Bureau of Investigation
FTO	Foreign Terrorist Organization
IMO	International Maritime Organization
ISW	Institute for the Study of War
JMIC	Joint Maritime Information Center
JNIM	Jama'at Nusrat al-Islam wal-Muslimin
UKMTO	United Kingdom Maritime Trade Operations
UAV	Uncrewed aerial vehicle
UFS	Ulchi Freedom Shield

Selected Sources

- Institute for the Study of War, Russian Offensive Campaign Assessment, 4 August 2026.
- Reuters, August 2026 reporting on Ukrainian strikes against Russian energy infrastructure and refinery incidents.
- Al Jazeera, 10 August 2026, reporting with AFP, Reuters and AP on Houthi missile and drone attacks against al-Makha, Yemen.
- Seneweb / AFP, 9 August 2026, on the JNIM-claimed attack against the Malian army camp at San.
- Al Jazeera and AFP, 11 August 2026, on the Kebbi firefight in northwestern Nigeria.
- Associated Press reporting carried by the Boston Herald, 10 August 2026, on the Ulchi Freedom Shield exercise announcement and North Korean missile activity.
- U.S. Department of State, 7 August 2026, "A New Era in U.S.-Colombia Relations."
- Reuters, 8 August 2026, on planned U.S. security assistance to Colombia's new government.
- El País English, 10 August 2026, on cartel violence spreading toward Mazatlán, Sinaloa.
- United Nations Security Council meeting coverage, 20 July 2026, on Haiti's road to elections and persistent gang violence.
- CISA, FBI and partner cybersecurity advisory AA26-222A, 10 August 2026, Gunra ransomware.

Method Note

This Weekly Security Briefing was prepared for S.F. Custos Global Reach Ltd. using open-source reporting available for the 3–10 August 2026 reporting week and later read-back checks conducted on 17 August 2026. Official, wire, United Nations, recognised analytical and reputable media sources were prioritised. Social-media and single-source claims were treated only as signals unless corroborated by official, wire or established analytical reporting. Assessments use calibrated confidence language and may change as additional reporting becomes available.