Intel News

OSINT SUMMARY – 16-31 July 2025

Compiled, researched & collated by @sif Iqb@l

- **Closure Threat to US Foreign Malign Influence Center Further Weakens Counter-Interference Efforts**
  A new legislative move threatens to close the Office of the Director of National Intelligence's Foreign Malign Influence Center (FMIC), the US government's primary hub for analyzing and coordinating intelligence on foreign interference. This follows earlier cuts impacting the State Department and FBI programs combating foreign influence. FMIC was established in 2022 and leads intelligence collection, partnerships, and analysis on threats to US democracy, including election security, from countries like Russia, China, and Iran. Its potential closure would diminish the nation's ability to coordinate a unified response to sophisticated foreign campaigns targeting US institutions, public opinion, and elections – a critical concern as adversaries employ increasingly advanced influence operations.

- **US State Department Suspends Intelligence Diplomacy Amid Bureau Abolition**
  As part of a broader reorganization led by Senator Marco Rubio, the US State Department has abolished a key bureau, ***Bureau of Intelligence and Research (INR)***, responsible for coordinating intelligence sharing with foreign governments, international entities, and non-governmental organizations. This bureau, which historically coordinated intelligence sharing with foreign governments and international organizations, has been shifted under a new Bureau of Emerging Threats that focuses on areas like cybersecurity and artificial intelligence. The restructuring has involved significant staff reductions and the consolidation or elimination of multiple offices, effectively putting a pause on certain intelligence diplomacy functions traditionally handled by INR. The reorganization aims to streamline operations but has raised concerns about its impact on intelligence cooperation and the ability to manage sensitive international security partnerships.
  This move effectively puts US intelligence diplomacy on hold, potentially impacting collaborative efforts in counterterrorism, cybersecurity, and global security partnerships. The decision raises concerns about the future of intelligence cooperation and information exchange critical to addressing transnational threats. It reflects a shift in US foreign policy and bureaucratic restructuring with significant implications for international intelligence alliances.

- **Washington's China Hawks Push for Stronger Intelligence Sharing with Europe to Counter Beijing's Influence**
  Amid perceived weakening of US capabilities to counter foreign interference and policy reversals under President Donald Trump, hawkish members of the US Congress are intensifying efforts to strengthen intelligence collaboration with European allies. The aim is to more effectively counter Beijing's expanding influence and covert operations across Europe. This congressional push emphasizes improving transatlantic coordination and intelligence sharing to thwart Chinese interference in political, economic, and technological sectors. The initiative reflects growing bipartisan concern over China's strategic ambitions and the need for a united Western response to safeguard democratic institutions and critical infrastructure from foreign manipulation.
  The news about Washington's China hawks pushing for stronger intelligence sharing with Europe to counter Beijing's influence dates from mid-2025, with significant developments reported around May and June 2025. Discussions and efforts intensified particularly following Chinese cyberattacks on

European institutions and increased concerns over China's strategic investments and influence in Europe during this period.

- **US Navy's Secretive SWORD Unit Tracks China's Underwater Drone Expansion**

  The Office of Naval Intelligence's covert SWORD unit is intensifying efforts to detect Chinese underwater drones operating in the Pacific. These advanced drones are believed to gather acoustic signatures from US submarines, posing a growing threat to American naval stealth and security. The unit's discreet operations reflect heightened US concerns over China's expanding capabilities in deep-sea surveillance and submarine tracking, critical elements of maritime dominance and intelligence gathering in contested waters.

  China's drone deployments in recent months have notably increased, especially in areas near US and allied submarine patrol routes. Detecting these drones is vital to preserving the stealth advantage that underpins US Navy deterrence and power projection. China's drone fleet is rapidly advancing, leveraging satellite-linked communications, integrated surveillance networks, and AI-driven navigation, enabling real-time data relay and broad area monitoring capability. The SWORD unit works to identify, track, and sometimes interfere with these underwater systems, preventing data collection that could compromise American undersea assets. The "SWORD unit" is a specialized sub-unit within the Office of Naval Intelligence (ONI), specifically focusing on HUMINT (Human Intelligence) operations. Breakdown of what SWORD entails:

  - ***HUMINT:*** SWORD specializes in covertly gathering intelligence from individuals and organizations.
  - ***Integration with JSOC:*** SWORD units are involved in supporting Joint Special Operations Command (JSOC) missions.
  - ***Specialized Skills:*** Personnel within SWORD possess advanced skills in areas like surveillance, counter-surveillance, interrogation, and deception.
  - ***Counter-Intelligence:*** Protect ONI and naval assets from enemy intelligence operations.
  - ***Information Warfare:*** ONI, as a whole, is heavily involved in information warfare, and SWORD contributes by gathering intelligence that informs these efforts.

- **UK Review Highlights Risks of Dependence on US Intelligence Amid Escalating Iran Threat**

  British Members of Parliament (MPs) have expressed serious concerns about the United Kingdom's vulnerability stemming from its reliance on US intelligence, particularly as threats from Iran increase. Their inquiry, conducted even before Donald Trump's return to the White House, underlines fears that overdependence on American intelligence-sharing could leave the UK exposed if priorities between London and Washington diverge or if US policy shifts unexpectedly.

  Recent intelligence assessments confirm Iran as one of the gravest state-based threats to the UK, with Tehran escalating its willingness to conduct espionage, cyber-attacks, and even physical operations on British soil. The official UK parliamentary report stresses the need for Britain to improve its own intelligence resilience and cyber defences, urging a fundamental review of strategy in the face of a rapidly evolving Iranian threat.

- **Western-Backed Justice NGO Engages Syria with War Crimes Evidence Amid Transitional Government**

  Following cautious recognition of the transitional government of Ahmed al-Sharaa by Washington and London, the Commission for International Justice and Accountability (CIJA) has begun direct engagement with authorities in Syria. The CIJA holds an extensive collection of intelligence documents detailing war crimes and human rights abuses committed during Syria's conflict. It aims to collaborate closely with the new rulers on accountability processes and to facilitate regular access to conduct on-ground investigations. This engagement comes amidst efforts to address past violations, clarify the fate of thousands of missing persons, support victim reparations, and lay groundwork for transitional justice in Syria. The cooperation represents a significant step toward international-backed justice mechanisms working with Damascus after years of conflict and sanctions.

  CIJA and similar NGOs possess a highly credible and vast collection of evidence documenting war crimes in Syria, including Damascus. Their evidence is sourced from multiple avenues that include photographic evidence, testimonies and interviews, official documents, international investigations from organizations such as Human Rights Watch, Amnesty International, and the UN Commission of Inquiry.

- **Israeli Air Strikes Undermine Ongoing Israel-Syria Normalisation Talks**

  After weeks of active negotiations for normalising relations between Israel and Syria, facilitated by the United States and involving the UAE, recent Israeli air strikes on Syrian infrastructure have cast doubt on the progress. Talks aimed at security coordination and confidence-building, marking the first direct engagement in over a decade, have been thrown into question. These military actions reinforce longstanding tensions and threaten to derail efforts to establish a formal peace or non-aggression agreement, despite underlying mutual interests such as countering Iranian influence in the region. The developments underscore the fragile nature of Middle East diplomacy where military actions can quickly reverse diplomatic advances.

- **Extensive Israeli Intelligence Operations Inside Iran Resulting in Iranian Counterintelligence and Internal Security Clampdown**

  During the period (16-31 July 2025), open-source reports confirmed that Israel continues to conduct highly sophisticated intelligence operations within Iran, developed over years. Israeli intelligence (Mossad) has penetrated large segments of Iran's security apparatus, enabling the targeting of military sites, key nuclear facilities, and high-ranking Iranian military officials. These operations involved a combination of human intelligence assets and artificial intelligence-guided attacks, including the smuggling of drones into Iran for precise strikes. The resulting impact severely weakened Iran's air defence and missile capabilities, highlighting Israel's long-term strategic focus on curbing Iran's nuclear ambitions and military power.

  In response to the revealed Israeli infiltration, Iranian authorities intensified internal security measures in July. These included detentions and charges of espionage against suspected Mossad collaborators within Iran, restrictions on electronic device usage by officials to prevent Israeli cyber intrusions, and urging citizens to report suspicious property leases possibly connected to Israeli operatives. This crackdown reflected Iran's growing concern over the depth and persistence of Israeli intelligence penetration and signalled a heightened state of alert to guard against ongoing covert threats.

- **Strategic Implications for Regional Stability:** OSINT analysis during this timeframe suggests significant shifts in regional dynamics. The extensive Israeli intelligence campaign and subsequent military actions against Iran have reinforced perceptions of Iran's vulnerability and have intensified concerns about regime stability. The political and military repercussions weaken Iran's position and complicate its ability to project influence in proxy conflicts. Moreover, the overt nature of Israeli public disclosures about their intelligence capabilities serves psychological warfare to publicly undermine Iranian morale and deter further aggression. The 2nd half of July 2025 marks a continued escalation in intelligence and covert activities, demonstrating the intertwining of human intelligence, cyber warfare, and advanced technology shaping the Israel-Iran confrontation.

- **Mossad Operations**

  During the latter half of July 2025, Mossad, Israel's premier intelligence agency, reportedly intensified secretive operations across multiple regions beyond Iran, continuing its established global intelligence and covert action footprint. Mossad activities fit a broader strategy that integrates cyber intelligence, drone technology, human intelligence, and psychological operations to maintain an edge in intelligence and security globally. The following elaboration is synthesized from available OSINT and historic intelligence operation patterns to inform ongoing situational awareness for the period of OSINT:

  - **Coordinated Operations in Strategic Regional Locations:** Mossad undertook covert attacks and intelligence-gathering missions not only inside Iran but also in key locations where Iranian influence and hostile groups operate. These include ongoing activities in neighbouring countries such as *Syria* and *Lebanon*, aimed at disrupting Iranian proxy networks and Hezbollah. Increased aerial surveillance and electronic monitoring along Israeli borders, including the Syrian frontier, reportedly supported these covert operations.
  - **Utilization of Collaborators and Local Assets:** The agency exploited local collaborators and "sayanim" – sympathetic individuals providing logistical support – allowing Mossad to conduct extensive operations with a lean budget while maintaining operational depth globally. In Iran, cells focused on smuggling weapons and collecting actionable intelligence. Similar tactics are assumed to be employed in other theatres where Israeli interests face threats.
  - **Kidnapping and Interrogation Tactics:** Across international locations, Mossad reportedly continued past patterns of capturing or neutralizing key adversaries through abductions and targeted killings often involving complex undercover operations. While no specific new major kidnappings or assassinations were publicly confirmed in this period, historical patterns suggest ongoing covert actions aligned with Israel's strategic priorities against Hamas, Hezbollah, and Iranian operatives abroad.
  - **Intelligence for Counterterrorism and Preventive Security:** Mossad actively gathered intelligence to pre-empt threats, including tracking weapon shipments and disrupting militant plans. These activities often involved collaboration with allied intelligence services and targeting sensitive infrastructure and logistics networks globally, ensuring Israel's proactive defence posture.

- **Emposat's European Satellite Networks Raise Espionage Fears Amid Chinese State Links**
  European intelligence agencies, including France's military security and Czech intelligence, are increasingly alarmed by the presence of satellite communication stations operated by Chinese telecoms group Emposat. The company is viewed as maintaining close ties with the Chinese government and Beijing's strategic priorities. Concerns center on the risks of espionage, surveillance, and data interception, highlighting broader strategic vulnerabilities when foreign-controlled critical telecom infrastructure is embedded within Europe. Recent actions, such as blocking Emposat's investments over spying fears, underscore the elevated scrutiny and geopolitical tensions surrounding Chinese tech influence in Europe's communications sector.

- **Beijing Revives Dialogue with Europe Amid Leadership Succession Debates**
  Chinese President Xi Jinping met senior European representatives in Beijing, signalling a renewed effort to stabilize and preserve Sino-European relations. This diplomatic engagement comes amid mounting internal debates over Xi's succession and leadership direction ahead. Reports confirm that the discussions focused on strengthening bilateral relationships, economic cooperation, and addressing mutual concerns amid the political context of Xi Jinping's upcoming succession debates within China. The unprecedented internal compromise within China aims to balance domestic political considerations while maintaining crucial ties with Brussels, reflecting Beijing's strategic priority to manage foreign relations carefully as it navigates an uncertain political transition. This move marks a significant reopening of dialogue after a period of strained ties between China and Europe and reflects Beijing's active effort to maintain stable and constructive ties with Europe during a sensitive period of internal political transition.

- **China Strengthens Intelligence Operations in Afghanistan to Safeguard Strategic Interests**
  China significantly intensified the presence and activities of its Ministry of State Security (MSS) within Afghanistan. This strategic shift aims to reduce China's historical dependence on Pakistan's Inter-Services Intelligence (ISI) for regional intelligence, seeking direct engagement with Afghanistan's ruling Taliban leadership. Chinese intelligence efforts focus on establishing cooperative ties with the Taliban's own intelligence apparatus to enhance situational awareness and security control. The enhanced MSS operations are driven by China's urgent need to protect its economic and security interests in Afghanistan, particularly related to the Belt and Road Initiative (BRI) infrastructure projects traversing the region. Beijing views reliable, first-hand intelligence as vital to managing risks posed by terrorist groups, insurgencies, and political instability that could disrupt Chinese investments and border security.

  The intensified Chinese intelligence operations in Afghanistan are part of a broader, multi-year strategic engagement. China has been steadily increasing its intelligence, diplomatic, and security cooperation with Afghanistan since around 2012, with a key acceleration after the US withdrawal in August 2021. Beijing pragmatically accepted the Taliban regime and began developing direct intelligence ties with the Taliban, reducing reliance on Pakistan's ISI. The years 2023 to 2025 have seen further formalization of this relationship, including the establishment of Chinese diplomatic presence in Kabul and expanded intelligence cooperation focused on protecting China's economic interests and regional security. The spike in activities seen in July 2025 should be viewed as a peak or intensified phase within this ongoing timeline of engagement rather than a new initiative starting solely in this month.

This development marks a notable intensification of China's long-term strategy to secure its geopolitical foothold in Central and South Asia through a more autonomous and assertive intelligence posture directly within Afghanistan. It also signals China's desire to play an active role in shaping regional security dynamics by leveraging intelligence cooperation with the Taliban regime. Understanding these intelligence advances is crucial to analyzing Beijing's regional influence, risk management approach, and evolving bilateral relations with Afghanistan during this critical period.

- ***China's Security Concerns in Afghanistan****:* China's main intelligence priorities involve countering terrorism – particularly from groups threatening Beijing's Xinjiang region like the East Turkestan Islamic Movement (ETIM) – and ensuring border security. Protecting Chinese investments and citizens working in Afghanistan is central to its security strategy.
- ***Chinese-Taliban Intelligence Cooperation:*** In July 2025, China continues to build robust intelligence ties with the Taliban, including high-level meetings between Chinese intelligence agencies and Taliban officials. This cooperation aims to manage security threats and stabilize the environment for Chinese investments in Afghanistan.
- ***Regional Intelligence Dynamics Involving China, Russia, and Afghanistan:*** China and Russia are cooperating to provide political cover and likely intelligence support to Afghanistan's interim government concerning counterterrorism and regional security matters. This cooperation shapes the intelligence environment in the region, blending geopolitical and security interests.
- ***China's Strategic Use of Intelligence for Infrastructure Projects:*** China's intelligence efforts in Afghanistan are tied to protecting its strategic investments, such as infrastructure within the China-Pakistan Economic Corridor expansion toward Afghanistan. Intelligence activities support risk assessment and security management for these projects.

- **Russian Missile Strike Devastates Ukrainian Military Intelligence Training Camp**

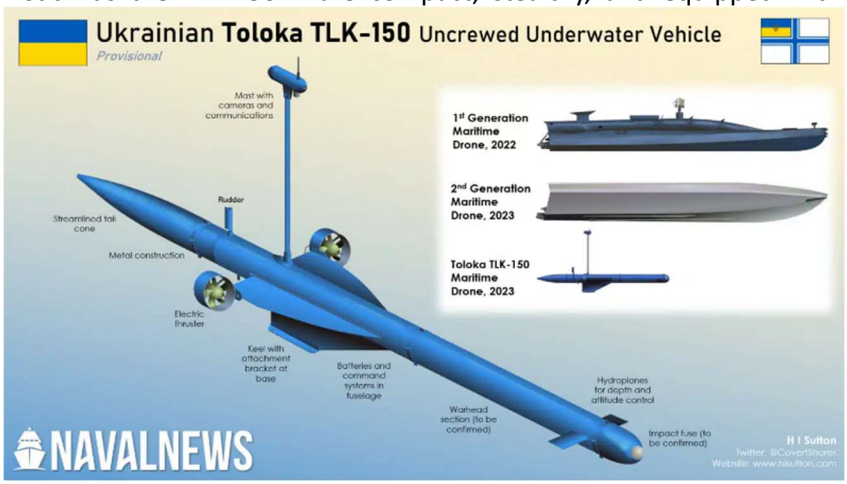
  On July 21, 2025, a Russian missile strike targeted a Ukrainian military intelligence training camp operated by the Main Directorate of Intelligence (GUR). The attack reportedly resulted in dozens of casualties, with Ukrainian sources confirming at least three soldiers killed and 18 injured, though Russian sources claimed much higher figures. The strike marked the latest in a series of aggressive attacks on Ukrainian military training facilities, aimed at weakening Ukraine's operational capabilities and morale. Ukrainian authorities launched an investigation to determine if any negligence contributed to the casualties and pledged to enhance troop security during training. This strike occurred amid escalating military tensions and ongoing conflict between Russia and Ukraine in 2025.

- **Russian Private Military Companies Española and Veteran Ramp Up Recruitment Amid Ukraine Losses**

  Following significant personnel losses in early summer during the conflict in Ukraine, Russian private military companies (PMCs) Española and Veteran – both linked to Russian military intelligence – have launched an intensive recruitment campaign. Targeting potential fighters online and at events in Moscow, these PMCs aim to replenish their ranks quickly to sustain operations on the Ukrainian front. The surge in hiring reflects Moscow's reliance on private military firms to supplement regular forces and maintain battlefield presence despite increasing attrition. This recruitment drive underscores the continued role of PMCs as critical proxies in Russia's hybrid warfare strategy and highlights the growing challenges in maintaining troop levels in the ongoing conflict.

- **FSB Declassifies WWII Archive on Volhynia Massacre to Stoke Ukraine-Poland Tensions**
  The Russian Federal Security Service (FSB) has released archival documents concerning the 1943-1944 Volhynia massacre, where thousands of ethnic Poles were killed by Ukrainian nationalist forces in what is now western Ukraine. This declassification appears strategically timed by Moscow to aggravate historical grievances and create diplomatic friction between Kyiv and Warsaw. By revisiting this painful chapter, Russia aims to undermine Ukrainian-Polish relations and weaken their unified stance against Moscow's geopolitical ambitions. The move is part of a broader Russian information campaign exploiting historical narratives to sow discord among EU and NATO allies in Eastern Europe. The release has elicited cautious diplomatic reactions, with Warsaw reaffirming its alliance with Kyiv despite the emotionally charged history.

- **Ukrainian Drone Maker Toloka Pursues Strategic Partnership with German Navy**
  Toloka, the Ukrainian drone manufacturer credited with supporting recent submarine strikes on Crimea's Kerch Bridge, is advancing talks to establish a strategic partnership with the German Navy. The collaboration aims to test and integrate Toloka's drone technology within NATO naval operations, enhancing Allied maritime capabilities. This move highlights Kyiv's innovative defence industry gaining recognition among Western military partners and underscores the increasing role of unmanned systems in contemporary naval warfare.
  Toloka's underwater drones – such as the TLK-150 – are compact, stealthy, and equipped with advanced navigation, surveillance, and secure communication systems. Capable of carrying significant payloads and operating covertly, these drones have set new standards in naval warfare by enabling long-range, precise, and cost-effective attacks. The TLK-150, for example, can deliver a 20–50 kg explosive payload over a range of up to 100km using cutting-edge stealth and manoeuvrability features.



- **Secretive D-2 Unit at Centre of Espionage Scandal Fuels Political Crisis in Kyiv**
  The highly secretive D-2 unit within Ukraine's National Anti-Corruption Bureau (NABU) has become the epicentre of an alleged espionage scandal shaking Kyiv's political landscape. Tasked with probing Ukraine's most sensitive and politically charged corruption cases, D-2 operates under a veil of secrecy, making it both influential and controversial. The D-2 unit is a highly secretive and elite subdivision within NABU. On D-2's functions and leadership:
  - The D-2 unit specializes in probing politically sensitive, high-level corruption cases.
  - It handles operations involving top officials, major financial crimes, and espionage linked to state actors.
  - Personnel are highly vetted and work under strict secrecy protocols.

- The head of NABU oversees D-2 directly, maintaining tight operational control.
- D-2 conducts covert investigations, gathers intelligence, manages covert informants, and collaborates closely with Ukraine's security services and prosecutors.

Recently, a major espionage scandal has erupted around the D-2 unit:

- An official within the D-2 unit was detained by the Security Service of Ukraine (SBU) and accused of spying for Russian intelligence. The suspect is alleged to have passed classified information, including data on Ukrainian law enforcement officers and sensitive investigations, to Russian operatives linked to the former security chief of ousted President Yanukovych.
- This spy allegedly helped facilitate planned Russian terrorist attacks and targeted operations against Ukrainian personnel.
- The investigation revealed that the spy's actions were coordinated by Dmytro Ivantsov, a former deputy head of Yanukovych's security who fled to Russia after 2014 and was recruited by the Russian FSB.
- Large-scale searches of NABU offices and employees followed, with complex accusations of internal leaks and collusion with hostile intelligence.
- NABU has launched an internal review contesting the basis and evidence behind the charges and expressed concern about the impact on anti-corruption work.
- The scandal highlights vulnerabilities in Ukraine's anti-corruption institutions amid the ongoing war and political pressure.

The unfolding espionage affair, involving accusations of leaking classified information or collusion with foreign intelligence, threatens to undermine NABU's credibility and deepen political tensions. This crisis highlights the fragile balance between anti-corruption efforts and political intrigue in Ukraine amid ongoing domestic and geopolitical challenges

- **Ukraine Counterintelligence Probes Infiltration of Sicarios Among International Legion Volunteers**

Ukraine's domestic intelligence agencies are investigating reports that Spanish-speaking volunteers, suspected to include cartel-affiliated sicarios, have infiltrated the International Legion fighting on the frontline. These individuals are believed to be recruited via private military companies to train in operating First-Person View (FPV) drones, which are increasingly used for reconnaissance and tactical strikes. Details on Sicario infiltration in Ukraine are elicited as under:

- ***Cartel-Linked Infiltration:*** Ukraine's counterintelligence services, prompted by warnings from Mexico's National Intelligence Center (CNI), are investigating reports that cartel-affiliated operatives – specifically Mexican sicarios – have joined the International Legion not for ideological reasons, but to gain combat experience and specialized training in the operation of FPV (First Person View) military drones. Some of these individuals are suspected of using false passports and recruitment by private military companies to mask their cartel affiliations.
- ***Scope of Training:*** Ukraine's rapidly evolving drone warfare environment has essentially turned the country into a global proving ground for tactical drone operations, attracting foreign fighters with criminal backgrounds seeking to learn advanced skills such as drone assembly, thermal camouflaging, electronic signal jamming, and low-altitude flight manoeuvres. These are tactics already being used by Latin American cartels for drug trafficking and targeted attacks back home.
- ***Notable Incidents:*** Among the trainees was an individual known as "Águila-7," a Mexican volunteer allegedly linked to Mexico's special forces and, by extension, to the Zetas cartel.

Ukrainian intelligence believes other individuals with similar backgrounds may have entered the country on Salvadoran, Panamanian, or Venezuelan documents.

- ***Security Measures:*** In response, Ukrainian authorities—working with international partners—are tightening security controls and monitoring documentation to identify and expel such infiltrators. However, the wartime environment and prevalence of forged papers complicate these efforts.
- ***Broader Implications:*** The United States and other partners have raised concerns that combat-proven drone tactics learned in Ukraine could be exported to criminal operations in the Americas, further empowering cartels to conduct hostile surveillance, smuggling, and violence with drone-delivered explosives. Ex-members of Mexican cartels have confirmed the growing use of FPV drones for both offensive and logistical criminal activities.

This convergence of organized crime and modern military technology highlights unintended consequences of the conflict, as Ukraine's frontline becomes a training ground for both international volunteers committed to Ukraine and transnational criminal organizations seeking advanced warfare skills. Likewise, they are potentially threatening the security and integrity of Ukraine's international volunteer forces. The probe underscores the complex challenges Ukraine faces in vetting foreign fighters amid the ongoing conflict and hybrid warfare environment.

- **Russia Expert Appointed to Lead French Military's Counter-Interference Unit**

  Colonel Guillaume Dufour, France's Russian-speaking defence attaché in Ukraine, has been appointed head of the Defence Ministry's "Strategic Anticipation and Orientation" unit. His role involves enhancing France's ability to predict and counter Russian interference and hybrid warfare tactics. Dufour's frontline experience and linguistic skills are crucial in interpreting evolving Russian strategies during the Ukraine conflict. His appointment dovetails with France's broader intent to deepen military intelligence capabilities that underpin its active role in supporting Ukraine and preparing for future security challenges in Europe. This illustrates the high priority France places on the Ukraine war as central to its strategic defence posture.

  President Emmanuel Macron and French policymakers emphasise that Ukraine's resistance is linked directly to Europe's future security. This has led to substantial military, humanitarian, and diplomatic support for Kyiv, including billions in aid, advanced weapons systems, and training programs. France also sees Ukraine's success as pivotal for maintaining NATO cohesion and preventing further Russian advances in Eastern Europe or beyond. The French government's strategic documents highlight Russia as the principal threat to France and Europe, with China also identified as a major challenge. The Ukraine war is thus seen as a proxy battleground that tests Western unity and resilience, shapes the regional balance of power, and affects global geopolitical alignments. France's engagement aims to ensure a just and lasting peace based on international law, which is essential for its own national security and European stability by 2030.

- **French Military Intelligence Taps La mètis for AI-Powered Analytics in Major Outsourcing Drive**

  France's military intelligence directorate has initiated a significant outsourcing program engaging 26 private sector companies to enhance its analytical capabilities. Among the targeted firms is ***La mètis***, a relatively new developer specializing in artificial intelligence-powered tools. This collaboration aims to modernize intelligence data processing and improve decision-making through advanced AI analytics. The outsourcing program reflects France's strategic shift towards integrating cutting-edge technologies from the private sector to bolster military intelligence effectiveness, operational agility,

and situational awareness. La mètis's participation underscores the increasing role of AI innovations in national security and defence intelligence modernization efforts.

- **French Foreign Ministry Engages Micro-Influencers to Amplify Communication Campaigns**
  The French Foreign Ministry's newly formed monitoring and strategy sub-directorate has adopted an innovative approach by enlisting micro-influencers to enhance its communication and information campaigns. This strategy aims to reach targeted audiences more effectively through trusted, niche voices on social media platforms, increasing the resonance and authenticity of France's diplomatic messaging. While this approach offers greater engagement potential and tailored outreach, it also carries risks related to message control, influencer reliability, and potential backlash. The move reflects a broader diplomatic trend toward leveraging digital and social media influencers to shape public opinion and counter disinformation in an increasingly complex information environment. France's adoption of micro-influencers signals an evolution in public diplomacy tactics to adapt to modern communication landscapes.

- **Macron's Upcoming Iraq Visit Focuses on Securing Major Defence and Trade Deals**
  French officials are preparing for President Emmanuel Macron's anticipated trip to Iraq this autumn, with a strategic focus on boosting bilateral trade relations. The visit aims to leverage France's strong defence sector to secure significant contracts and partnerships in Iraq's reconstruction and security modernization efforts. This initiative aligns with broader French ambitions to deepen economic and geopolitical ties in the Middle East, enhancing France's influence while supporting Iraq's stability through defence cooperation and infrastructure development.

- **French War College Academics Face Pay Cuts Despite Surge in Defense Budget**
  Although President Emmanuel Macron has pledged a historic increase in France's military budget – aiming to double defence spending to €64 billion by 2027 – academics at France's army war college are now experiencing reductions in remuneration for some of their duties. This move has emerged even as the government emphasizes the need for greater military strength in light of escalating security threats. The decisions signal a possible reprioritization of resources or fiscal tightening within military educational institutions, highlighting a disconnect between headline defence funding boosts and day-to-day academic support within strategy and officer training circles.

- **French Military Intelligence Arabic Teacher François D. Dismissed Over Espionage Allegations**
  François D., an Arabic language instructor with 26 years of service at the French Joint Intelligence Training Centre, was dismissed following an internal investigation that accused him of undisclosed links to Tunisian and Algerian intelligence agencies. While he contests the dismissal in court, the case highlights ongoing security concerns and counterintelligence measures within French military educational institutions, especially given France's complex intelligence relations with North Africa. This case also underscores heightened counterintelligence vigilance within French military education, especially regarding North African intelligence dynamics.

- **India Turns to New Space Initiatives to Close Earth Observation Intelligence Gap with China**
  India's Earth observation programs, primarily developed by the Indian Space Research Organisation (ISRO), have struggled to match the advancements of Chinese space intelligence capabilities. Despite

significant investments, India faces challenges in satellite coverage, data integration, and real-time intelligence utility compared to China's rapidly expanding space surveillance infrastructure. To address this gap, New Delhi is increasingly relying on "New Space" players – private companies and innovative space ventures – that offer agile, cost-effective satellite technologies and enhanced data analytics. This strategic pivot aims to bolster India's geospatial intelligence capabilities and regain competitive advantage in regional space-based surveillance crucial for national security and geopolitical positioning. The move also aligns with global trends where fast-evolving commercial space entities complement traditional government space programs to meet demanding intelligence requirements. For the US it is an issue that what it perceived India as a regional challenger to China, all perception till now has failed.

- **Emirati Missiles on Turkish Drones: PR Display Rather Than Real Integration**
  At the recent Turkish defence exhibition in Istanbul, Baykar, the leading Turkish drone manufacturer, showcased several missiles from Abu Dhabi's defence conglomerate. Although the display attracted significant attention, industry insiders and analysts suggest the exhibit was primarily a public relations move rather than evidence of actual missile integration on Turkish drones. Technical and operational compatibility challenges, as well as strategic considerations, indicate that full integration is not imminent. The exhibition appears designed to signal potential cooperation and foster political goodwill rather than announce concrete defence procurement or joint development programs. This case highlights the nuances in defence diplomacy where symbolic displays sometimes mask the true status of military-industrial partnerships.

- **Poland Secretly Tests US-Made Havoc AI Sea Drones in the Baltic Inspired by Ukrainian Tactics**
  Polish special forces from the elite JW Formoza unit have been conducting covert trials of autonomous naval drones developed by the US company HavocAI off Poland's northern coast near Gdynia. The exercises, inspired by Ukraine's military intelligence experience in the Black Sea, include night navigation, signals intelligence (SIGINT) collection, and infiltration scenarios. Poland is preparing to strengthen its maritime defence capabilities in the Baltic Sea, focusing on scalable, low-cost autonomous drone platforms that offer stealth, survivability, and networked operation for high-intensity conflict. The HavocAI drones can carry significant payloads and operate using solar panels, extending their mission endurance. This testing aligns with broader US-Poland technological cooperation amid rising tensions along NATO's eastern flank. HavocAI's strategic partnership with Lockheed Martin supports further development of these autonomous naval systems, reflecting growing Pentagon interest and congressional funding for AI-powered maritime platforms. Poland's trials mark a significant step in shifting naval warfare posture to counter regional threats effectively while minimizing personnel risk.

  Poland's adaptation of Ukrainian drone tactics emphasizes lessons learned from the ongoing conflict in the Black Sea, recognizing autonomous systems and swarm capabilities as essential for future maritime engagements. This move signifies Poland's commitment to enhancing NATO's eastern defences in a volatile security environment.

- **Polish Military Intelligence Closely Monitors Russian Spy Ship Almaz Nearing Completion in Kaliningrad**

  The Russian deep-sea intelligence vessel, Almaz, is in the final stages of construction at the Yantar Shipyard in Kaliningrad. Classified as part of the Main Directorate of Deep-Sea Research (GUGI), Almaz is designed for undersea reconnaissance, including surveillance of NATO submarine cables and strategic seabed operations. Polish military intelligence is deploying extensive resources to monitor the vessel's build, anticipate its deployment, and uncover details of its advanced intelligence-gathering technologies. The ship, alongside its sister vessels like Yantar and Vice-Admiral Burilichev, plays a critical role in Russia's underwater espionage efforts. This close surveillance reflects Poland's heightened alertness to Russian military activities in the Baltic region and the increasing strategic importance of undersea domains in intelligence and defence operations.

- **Karol Molenda: Poland's Cyber Defence Architect and Strategist on NATO's Eastern Flank**

  General Karol Molenda, Poland's cyber defence chief, is a pivotal figure driving the digital modernization of the Polish Armed Forces. Known as a quiet yet forward-thinking strategist, Molenda champions cutting-edge technologies such as artificial intelligence and quantum cryptography to enhance Poland's cyber resilience. He also spearheads offensive cyber doctrines to counter Russia's evolving hybrid and cyber threats. Positioned on NATO's critical eastern frontier, Molenda's leadership shapes Poland's efforts to bolster its national and alliance-wide cyber defence capabilities amid increasing regional tensions. His work reflects the broader strategic imperative to integrate advanced technologies for intelligence, defence, and deterrence in the modern security environment. Following are his achievements:

  - He was the ***first Pole to chair the Cyber Commanders Forum in 2022,*** demonstrating his recognition and influence internationally in cybersecurity leadership.
  - Molenda played a pioneering role in the ***creation of the Polish Cyber Command*** and the development of an advanced computer forensics laboratory.
  - Under his leadership, Poland's Cyber Defence Forces were established, developing a modern cyber defence architecture expected to reach full combat readiness by the end of 2024.
  - He supports integration of cutting-edge technologies such as ***artificial intelligence and quantum cryptography*** into defence strategies.
  - Molenda fosters international cooperation on cyber threats, representing Poland in NATO cyber exercises and global security conferences.
  - He received prestigious honours including the ***Army Commendation Medal from the U.S. Department of Defense*** and several cybersecurity awards such as the ***European CYBERSEC Award in 2021***.
  - Molenda emphasizes human resource development and innovative management models such as the NICE standard for cybersecurity.
  - He is known for his strategic vision in offensive cyber doctrines and enhancing Poland's resilience against hybrid threats from Russia.
  - His command oversees 24/7 monitoring and response capabilities, cryptology research, and public awareness campaigns on cyber security best practices.

- He holds advanced degrees in electronics and cyber security and has a strong background in military counterintelligence.

- **Monaco Plans Major Reform to Strengthen Its Internal Intelligence Service**
  Monaco's Interior Minister Lionel Beffre is spearheading efforts to reform and enhance the principality's Internal Intelligence Division (Division de Renseignement Intérieur; principality's sole intelligence agency responsible for domestic security and intelligence operations). Under growing international pressure due to evolving security challenges, Monaco recognizes the need to significantly upgrade the capabilities of its sole intelligence agency. The reform aims to modernize intelligence operations, improve threat detection and response, and align Monaco's intelligence framework with global standards. Government officials are also exploring wider structural reforms across the intelligence sector to bolster national security, counter espionage, and enhance cooperation with foreign partners. This initiative highlights Monaco's shift towards a more proactive and robust intelligence posture amid rising geopolitical and regional threats.

- **Vietnam's DG2 Trains Laotian Intelligence Students to Strengthen Regional Security Cooperation**
  Vietnam's Directorate General 2 (DG2), the military intelligence agency, has been actively involved in training Laotian spy students as part of expanding intelligence cooperation with Laos. This training initiative aims to enhance Laos's intelligence capabilities, particularly in human intelligence (HUMINT), counterintelligence, and regional security challenges. The program reflects deepening strategic ties between the two neighbouring countries, focusing on strengthening mutual surveillance, intelligence sharing, and operational coordination to address transnational threats and maintain stability in the Indochina region. This development underlines Vietnam's role as a regional security leader supporting allied intelligence growth in Southeast Asia.

- **Vietnam's Cybersecurity Unit A05 Protects State Secrets with Equipment Assembled in Croatia**
  Vietnam's Ministry of Public Security unit known as A05, responsible for cybersecurity and high-tech crime prevention, is employing equipment assembled in Croatia to track down those responsible for cyber leaks and breaches. This innovative use of commercial channels and international technology reflects Vietnam's growing cyber defence capabilities amidst increasing threats in cyberspace. Unit A05's proactive approach, combined with international cooperation and advanced technology, strengthens Vietnam's ability to safeguard state secrets and critical infrastructure from cyber espionage and attacks. This development marks a significant step in Vietnam's expanding cybersecurity strategy amid evolving digital threats.

Corporate Intelligence

- **London-Based G3 Expands Workforce Following New Investment**
  G3, a London-based firm, has initiated a recruitment drive after securing a new investor, signalling plans for growth and increased operational capacity. This infusion of capital is likely intended to support expansion efforts, enhance service offerings, or enter new markets. The move underscores confidence in the company's prospects amidst evolving industry dynamics and investor interest in the sector.
  G3 primarily operates as a strategic advisory consultancy specializing in intelligence, cyber security, risk mitigation, governance, and investigations, with clients including large corporations, investment funds, and law firms. It offers services such as strategic advice, due diligence, cyber security, reputational intelligence, and dispute resolution rather than armed military services or private military contracting. There is also a separate entity called G3 Security Services in London, which provides professional security guarding services (such as manned guarding and key holding) but not military combat or private military contracting typically associated with a PMC.

- **Russian Cybersecurity Firm Protelion Relocates Operations to Armenia While Maintaining US Presence**
  Protelion, formerly known as *Infotecs*, a Russian cyber provider, has strategically shifted its international operations base to Yerevan, Armenia, while retaining a footprint in the United States. The move allows Protelion to continue leveraging key personnel and maintain operational continuity amidst geopolitical pressures. This relocation reflects broader trends of Russian tech firms seeking more stable environments for international business amid increasing sanctions and restrictions, while balancing engagement with Western markets. Armenia's relatively neutral geopolitical stance makes it a preferred hub for such transitional operations in the cyber sector.
  Protelion specializes in advanced cybersecurity solutions focused on protecting digital communications and providing secure access in various environments. Their offerings include end-to-end encryption of traffic, endpoint protection, industrial security for manufacturing environments, and secure communication platforms that prevent insider threats and man-in-the-middle attacks. They emphasize ease of use, high performance, and innovative encryption key management.
  There is no publicly available information or credible evidence suggesting that Protelion provides direct support to the Russian military and apparently their focus is on cybersecurity products and services for businesses and industrial clients only.

- **Corporate Intelligence Experts Return to Damascus Amid Improving Security and Reconstruction Efforts**
  As security conditions in Syria gradually stabilize, corporate intelligence specialists – particularly those focused on geopolitical risk and investigations – are reestablishing their presence in Damascus. Their return aligns with increased activity from international donors and organizations involved in Syrian reconstruction. These intelligence professionals aim to monitor the evolving political landscape and gather insights on the inner workings of the new regime, helping clients navigate the complexities and risks associated with investment and rebuilding efforts in the country. This development signals cautious optimism about Syria's future while underscoring ongoing uncertainties.

- **PwC Faces Suspension from Saudi Arabia's Public Investment Fund, Defence Business at Standstill**
  PwC's Saudi defence consulting arm has been effectively paused after the kingdom's sovereign wealth fund, the Public Investment Fund (PIF), imposed a temporary ban on awarding it advisory and consulting contracts until February 2026. The suspension also extends to PIF's more than 100 subsidiaries, severely restricting PwC's operations in one of the Middle East's fastest-growing markets. Although PwC denies a formal ban and attributes the issue to a "client matter," investigations are reportedly underway into at least one of its contracts with PIF.
  PricewaterhouseCoopers (PwC) is one of the world's largest professional services firms, offering assurance, tax, and consulting services globally. is a multinational professional services network headquartered in London. It is considered one of the "Big Four" accounting firms globally, providing extensive auditing, assurance, consulting, tax, and advisory services to large corporations, governments, and institutions. PwC's expertise often spans multiple sectors including finance, healthcare, technology, and defence, making it a leading adviser for complex economic transformations worldwide. It played a significant role in Saudi Arabia's Vision 2030 economic diversification by advising on major projects, including defence modernization. This suspension risks delaying key initiatives within the kingdom's defence sector, which is undergoing rapid transformation driven by large U.S. arms deals and local industrialization efforts. PwC is actively seeking to restore relations with PIF to resume its crucial advisory role in Saudi Arabia's strategic projects.

- **Prince Faisal bin Bandar Al Saud: The Gamer Prince Driving Saudi Arabia's Esports Revolution**
  Prince Faisal bin Bandar bin Sultan Al Saud is a key figure in the development of Saudi Arabia's esports and gaming industry. Serving as the President of the Saudi Esports Federation (SEF) since 2017 and Vice President of the Global Esports Federation since 2021, he has significantly expanded the Kingdom's role in the global gaming ecosystem. Prince Faisal is known for his passion for gaming and his strategic vision to transform esports into a professional and sustainable industry in Saudi Arabia. He pioneered major initiatives like the Gamers8 festival, the world's largest esports event, held annually in Riyadh, positioning Saudi Arabia as a global esports hub. Alongside promoting gaming, he emphasizes the cultural potential of video games to tell Arab stories and foster community development. Prince Faisal also holds influential positions in his family's business ventures, linking traditional royal interests with modern digital entertainment industries. His leadership is central to Crown Prince Mohammed bin Salman's vision of diversifying and modernizing the national economy through innovative sectors like gaming and technology.

- **Prince Khalid bin Bandar Set to Return to Business Amid Saudi Embassy Departure**
  Prince Khalid bin Bandar bin Sultan al-Saud has recently concluded his six-year tenure as Saudi Arabia's ambassador to the United Kingdom. His diplomatic period has been widely recognized as a transformative phase marked by renewed engagement and modernization of Saudi-UK relations across political, economic, academic, and cultural fields. Prince Khalid actively promoted Vision 2030 reforms, significantly enhanced bilateral trade and cultural ties, and improved Saudi Arabia's image in the UK through transparent and accessible diplomacy. Before his ambassadorial appointment in 2019, Prince Khalid had a successful career in business, particularly in the defence sector. The business group he founded, ***Dayim Holdings***, recently secured investment from one of Moscow's largest funds, whose leadership faces Western sanctions, highlighting complex geopolitical financial entanglements.

Following his ambassadorial role, he has been appointed as an advisor to the Saudi Ministry of Foreign Affairs and is expected to return to Riyadh. This move is anticipated to allow him to refocus on his business interests, particularly in defence and international investments, at a time when his company is further integrated into complex geopolitical finance networks. Overall, his departure signals a potential shift back to leveraging his commercial and defence expertise amid continued strategic manoeuvring between regional and global powers.

Dayim Holdings, founded in 2006, is primarily an investment and strategic partnership group focused on various sectors across the Gulf region. While it is not a direct defence manufacturer, Dayim is increasingly involved in defence-related activities through equipment rental services and strategic joint ventures. The group participates in defence industry events and supports the expanding Saudi Arabian defence ecosystem, aligning with the kingdom's Vision 2030 goals to localize and grow its military industries. Thus, Dayim Holdings maintains a foothold in the broader defence sector, mainly as an investor and service provider rather than a direct defence contractor.

- **RedSense Files Lawsuit Against Former Cyberthreat Intelligence Chief for Trade Secret Theft**
  Cybersecurity firm RedSense has initiated legal proceedings against its former Chief Research Officer, Yelisey Boguslavskiy, alleging multiple serious offenses including theft of trade secrets and breach of fiduciary duty. Boguslavskiy, known for his media presence and cybersecurity expertise, is accused of misappropriating proprietary research and confidential information to benefit competitors or personal ventures. The lawsuit highlights ongoing challenges within the cybersecurity industry regarding protection of sensitive threat intelligence and the risks posed by insider threats. RedSense's move underscores the increasing legal and reputational stakes for firms operating in the competitive and strategically critical field of cyberthreat intelligence.

- **Elon Musk Associate Chris Gober Launches Maven Defense Solutions Targeting US Administration**
  Chris Gober, known for his close association with Elon Musk, has founded Maven Defense Solutions, a new consulting firm focused on the defence sector. The company seeks to leverage Gober's influential connections within the current US administration to secure contracts and advisory roles. Maven Defense Solutions aims to navigate complex defence procurement landscapes and offer strategic intelligence and consulting services tailored to government clients. This venture reflects a growing trend of technology insiders and politically connected entrepreneurs entering the defence industry to shape policy and business outcomes. Gober's involvement underscores the intersection of high technology, political influence, and defence consulting in Washington.

- **Former CIA Chief of Staff and Project 2025 Intelligence Author Joins Meta in Key Strategic Role**
  John Ratcliffe's former chief of staff at the Office of the Director of National Intelligence (ODNI), ***Dustin J. Carmack,*** who authored the intelligence section of Project 2025, has assumed a top strategic position at Meta. Project 2025, a comprehensive 900-page policy roadmap developed by the conservative Heritage Foundation, outlines a radical agenda for reshaping the federal government and consolidating executive power under a second Trump administration. The associate's

move to Meta reflects a strategic bridging of high-level intelligence expertise and private sector technology leadership, highlighting the growing influence of political and intelligence actors in major tech firms. Project 2025 itself has been influential in shaping right-wing policy and personnel decisions within the Trump administration.

- **Former DHS Counterterrorism Chief Matthew Wortzel Joins Private Security Sector**
  Matthew Wortzel, formerly the Assistant Secretary for Counterterrorism and Threat Prevention at the US Department of Homeland Security, has transitioned to a strategic position in the private security industry. This transition highlights the ongoing trend of high-ranking government counterterrorism officials bringing their expertise to private industry, where they advise on homeland security, threat mitigation, and risk management.
  Renowned for his expertise in counterterrorism strategy and intelligence, Wortzel's move underscores the growing integration of government-honed security competencies into private sector risk management and threat mitigation frameworks. His role is expected to deepen partnerships between corporate security and government counterterrorism efforts, enhancing the capability to anticipate and respond to evolving terrorist threats.

- **Assassination Attempts and Hangar Seizures Highlight Tense Arms Trade in Guyana**
  In Guyana, the role of local defence representatives in the burgeoning arms market has become fraught with danger and intrigue. As Guyana emerges as a new oil-rich frontier in South America, its arms markets have attracted intense interest amid escalating tensions with neighbouring Venezuela. The environment is marked by violent tactics including assassination attempts and hangar seizures, reflecting the high stakes involved in controlling regional arms supplies.
  The brokering landscape in Guyana's arms trade is a mix of local powerful defence representatives who use heavy-handed methods, backed by international interests, chiefly the US, aiming to counterbalance regional threats and influence security dynamics.
  - The US government and military are actively enhancing cooperation with Guyana, including joint naval exercises and intelligence sharing.
  - US companies involved in broader defence contracts and infrastructure projects in the Caribbean region include major contractors like Lockheed Martin, Raytheon, and others active under Department of Defence contracts. These firms typically supply advanced weapons systems, sensors, and support services.
  - Sincerus Global Solutions is a defence services company mentioned in connection with Guyana-related defence reform programs, with individuals such as Grimes reportedly paid by them.
  - The US Department of Defence awards various contracts (not necessarily specific to Guyana but in the region) to multiple firms for construction, logistics, maritime, and technology services.

  Guyana's recent discovery of oil wealth has heightened regional tensions, particularly with neighbouring Venezuela, leading to fierce competition among local defence brokers and representatives. These brokers navigate a volatile landscape where control over arms supplies is linked to power and influence, employing violent tactics to secure their stakes. This complexity is compounded by Guyana's efforts to strengthen its security infrastructure amid geopolitical rivalries, attracting the attention of Western and regional actors seeking to monitor and manage arms proliferation. Such a volatile context presents multifaceted challenges involving illicit arms flows, corruption, and political violence, all of which risk destabilizing Guyana's fragile security environment.

The situation reflects the intersection of commercial interests, regional power struggles, and the risks borne by brokers and officials in managing these high-stakes defence transactions.

- **Liberia Engages Discreet Seychelles Trust for US Lobbying Efforts Outside Formal Diplomatic Channels**
  Liberia is employing a discreet trust based in Seychelles, ***Emerald Global Investments***, to conduct lobbying activities in the United States, circumventing traditional diplomatic pathways. This move reflects Monrovia's strategic effort to establish influence and direct communication with US politicians and diplomats through private and less transparent channels. Given Liberia's complex political and economic challenges, leveraging offshore entities for lobbying purposes highlights a trend of non-traditional diplomatic engagement aimed at securing international support, investments, and political backing. The use of a Seychelles-based trust, known for its opacity, underscores challenges in transparency and governance in Liberia's external relations strategies. This approach also aligns with broader patterns of smaller states seeking alternative means to navigate global power centres.

- **UAE Military Dramatically Cuts Back on Foreign Consulting Firms, Focusing on Domestic Solutions**
  The United Arab Emirates armed forces are significantly reducing the number and value of contracts awarded to foreign consulting firms as part of a strategic shift towards domestic capabilities. This move reflects the UAE's growing confidence in its own defence and technology sectors, as well as cost-control efforts amid evolving geopolitical and economic priorities. The reduction in reliance on foreign consultants signals a maturation of the UAE's military-industrial complex, aligning with broader national ambitions for self-reliance and local innovation. While the Gulf consulting market remains robust, the defence sector is increasingly favouring in-house expertise and local partnerships. This trend is reshaping the consulting landscape in the region, posing challenges to international firms that have historically thrived on public sector engagements in the Gulf.

- **Czech Firms Strengthen Kyiv's Drone Capabilities Through Commercial Partnerships**
  A commercial collaboration between Czech and Ukrainian companies exemplifies Prague's expanding role in supporting Ukraine's armed forces with advanced drone technology. Czech firms are supplying both reconnaissance and attack drones, enhancing Kyiv's battlefield intelligence and strike capabilities. This partnership underscores the strategic importance of Eastern European defence industries in the Ukraine conflict and highlights the Czech Republic's growing position as a critical supplier of unmanned aerial systems. The channel facilitates faster delivery, technology transfer, and operational support, reflecting broader Western efforts to equip Ukraine with modern, versatile military assets to counter Russian advances effectively. This connection also illustrates how commercial channels supplement government aid to bolster Ukraine's defence capabilities.

- **Bulgarian Court Case Uncovers Russian Oligarch-Tied Broker's AML Violations**
  Bulgarian authorities have fined Intercapital Markets (ICM) for violations of anti-money laundering (AML) regulations, shedding light on the firm's operations and its links to Russian oligarchs. Suleiman Kerimov (also sometimes spelled Souleiman Kerimov) is identified in multiple sources as a high-level Russian oligarch with ties to Bulgarian brokerage operations, including those under recent scrutiny. Suleiman Kerimov is a prominent Russian billionaire, oligarch, philanthropist, and politician with close ties to Vladimir Putin's government. He has major investments in various sectors including metals,

finance, and energy, and has held significant stakes in companies like Gazprom, Sberbank, and Polyus Gold – the largest gold producer in Russia. Kerimov has been under international sanctions by the US, EU, and UK since 2018 and particularly following Russia's invasion of Ukraine in 2022 due to his close ties to the Kremlin.

Regarding the link to ICM, Kerimov is connected to the brokerage through complex financial networks and intermediaries. Bulgarian authorities' court cases and investigations into ICM revealed that the firm was involved in operations benefiting politically exposed persons (PEPs) linked to Kerimov's financial empire. ICM has been fined for anti-money laundering (AML) violations, with evidence suggesting that it facilitated financial transactions for entities tied to the oligarch and his network, thus enabling covert money flows and asset management under scrutiny.

The case exposes mechanisms used by the broker to facilitate illicit financial flows, highlighting ongoing challenges in combating money laundering in Eastern Europe. ICM's politically exposed persons raises concerns over regulatory oversight and the effectiveness of AML enforcement in the region. The court case provides insight into the complex networks enabling financial crimes connected to Russian elite interests, underscoring the importance of continued vigilance and cross-border cooperation to disrupt such illicit activities.

- **Spectacular Revenue Growth for Moscow-Linked Aviation Subcontractors Siam Aero and Sky Kingdom in Bangkok**

  Reportedly, there is a remarkable surge in turnover for Siam Aero and Sky Kingdom, two aviation subcontractors based in Bangkok with links to Russian aviation networks. These companies, involved in aircraft maintenance, parts distribution, and aviation support services, have experienced unprecedented revenue growth within a short period. Sky Kingdom, led by seasoned professionals, is expanding its operations and participating in major industry forums such as Aero Engines Americas 2025. The rapid financial rise highlights increasing Russian influence in Southeast Asia's aviation sector and the strategic positioning of these firms within regional aircraft maintenance and technical service markets. Their growth reflects a broader pattern of Moscow-linked enterprises deepening commercial footprints beyond traditional spheres under shifting geopolitical dynamics.

- **China's Global AI Governance Initiative and Technological Intelligence Diplomacy**

  China took a major step in advancing its intelligence-related global technology agenda by announcing a comprehensive ***Action Plan for Global Artificial Intelligence (AI) Governance*** at the World Artificial Intelligence Conference (WAIC) held in Shanghai from July 26-28, 2025. Key intelligence-relevant points include:

  - The plan emphasizes ***international cooperation*** on AI development, governance, and security standards, aiming to preempt technological monopolies by a few countries or corporations.
  - China proposes establishing a ***new global AI cooperation organization***, potentially headquartered in Shanghai, to coordinate international AI regulatory frameworks and foster shared technology innovations.
  - This initiative reflects China's broader intelligence and technological diplomacy strategy to shape rules around AI—a critical emerging domain for state intelligence and national security capabilities.

- China stresses ***bridging the global intelligence divide***, especially aiding developing nations ("Global South") in accessing AI technologies for inclusive growth, enhancing its influence over the global tech ecosystem.
- Premier Li Qiang highlighted risks related to AI security, talent exchange barriers, and supply chain vulnerabilities, underscoring China's intent to safeguard critical AI infrastructure and knowledge.
- The event also featured Huawei's launch of its advanced AI computing system "CloudMatrix 384", signalling China's drive to compete at the forefront of AI hardware technologies important for intelligence operations.

This global AI governance push represents a significant dimension of China's state intelligence efforts – merging technological innovation, global regulatory leadership, and geopolitical strategy in shaping future intelligence environments. It also illustrates China's expanding intelligence reach beyond traditional domains into cutting-edge technology governance, which is pivotal in the emerging era of digital and artificial intelligence-driven intelligence and security operations.

- **China's Foreign Minister Wang Yi Engages US Business Leaders**

  In Beijing, on 30 July 2025, China's Foreign Minister Wang Yi held high-level meetings with leading executives from major US corporations, including Goldman Sachs, Boeing, and Apple. The discussions focused on promoting enhanced Sino-US engagement and emphasizing the importance of avoiding confrontation between the two global powers. This engagement highlights China's strategic approach to managing the multifaceted intelligence, economic, and geopolitical risks that define the complex bilateral relationship. The meeting indicates a proactive phase in China-US relations where economic ties and intelligence considerations are closely intertwined, and it serves as a critical diplomatic manoeuvre aimed at stabilizing one of the world's most consequential geopolitical relationships.

  Wang Yi's outreach to influential US business leaders underscores Beijing's intent to maintain open communication channels with key economic stakeholders and reduce tensions ahead of anticipated high-level leader summits later in the year. This effort reflects China's broader diplomatic and intelligence-driven strategy to balance competition with cooperation, safeguard its economic interests, and influence US policy through private-sector engagement.