GRYPHON GROWL

AFLCMC INTELLIGENCE CENTER OF EXCELLENCE (ICE)
INTELLIGENCE OPERATIONS FLIGHT: DSN: 713-0409 / COMM: 937-713-0409
FOR COMMENTS, PLEASE CONTACT: AFLCMC21IS.INO_ALL@US.AF.MIL

February 9, 2026

CONTENTS

The Gryphon Growl is a collection of news reporting produced by the 21st Intelligence Squadron and is designed to make acquisition professionals and leaders more fully threat informed. Articles are chosen because they impact AFLCMC programs or address larger national security issues in line with the Interim National Security Strategic Guidance, National Defense Strategy, Reoptimizing for Great Power Competition, and AFMC/AFLCMC priorities. The Gryphon Growl is designed to generate discussions in your respective workspace on current events. If any topic drives interest at higher classifications, please contact your PEO's Director of Intel or the ICE, using the phone number listed above or at https://usaf.dps.mil/sites/21IS. The articles in this product are gathered from unclassified, open sources and are not evaluated intelligence products. The included articles do not reflect the official position of the 21 IS, AFLCMC, or DoD.

For additional 21IS reporting, use the URLs below to access the 21 IS Inteldocs & ICE Page on SIPR & JWICS

SIPR
go.intelink.sgov.gov/CPI6RmN
Current Intelligence Brief (Monthly)

JWICS
go.intelink.ic.gov/3vKnmH3
AFLCMC CC Intel Brief (Monthly)
Winged Warrior (Bi-Weekly)
CyREN (Bi-Weekly)

Gryphon Growl Feedback Form: https://forms.osi.apps.mil/r/WhpBtWbWYi

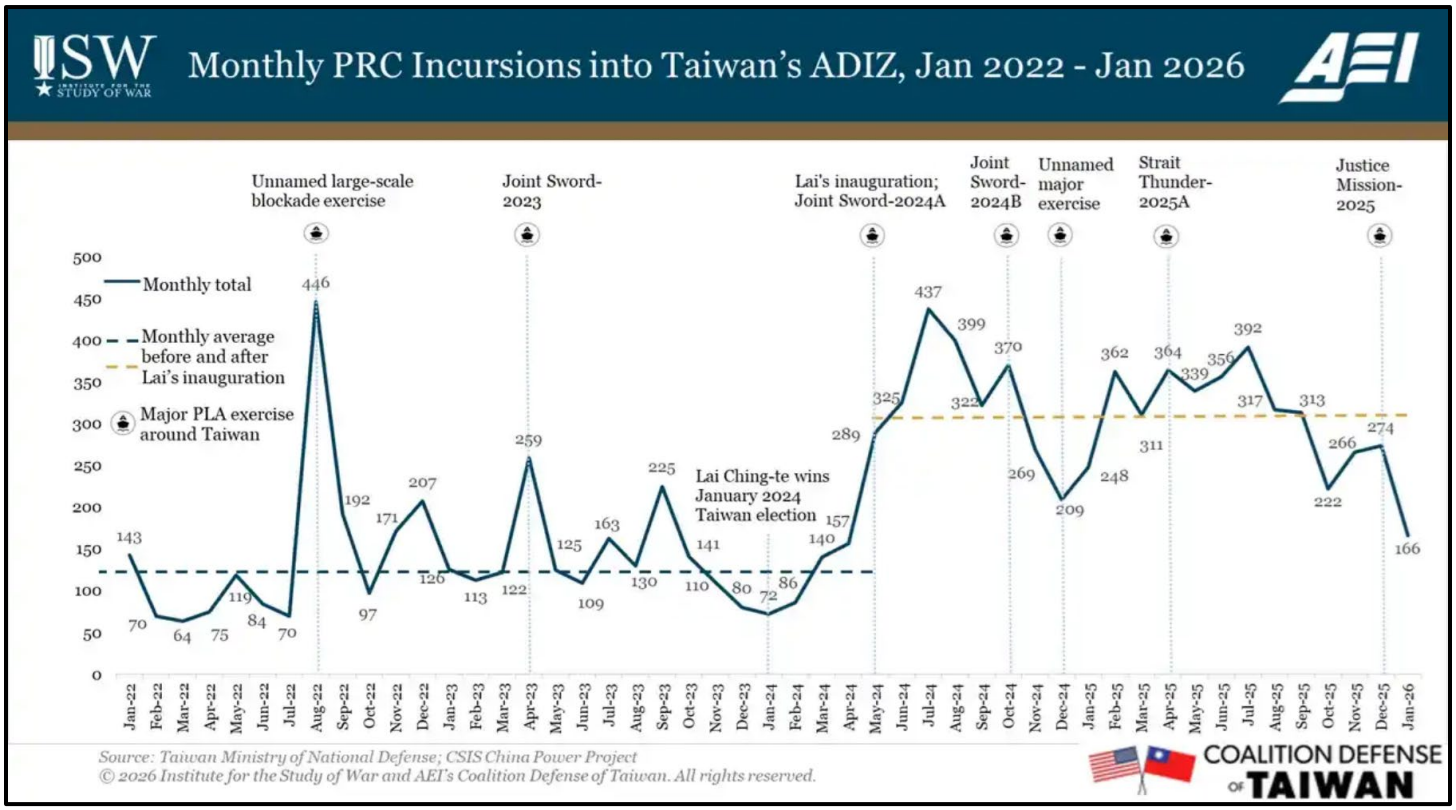
We value your thoughts on the Gryphon Growl—share them with us!
Your input helps improve and enhance our product.

INDOPACOM

ISW: CHINA-TAIWAN UPDATE

Key Takeaways:

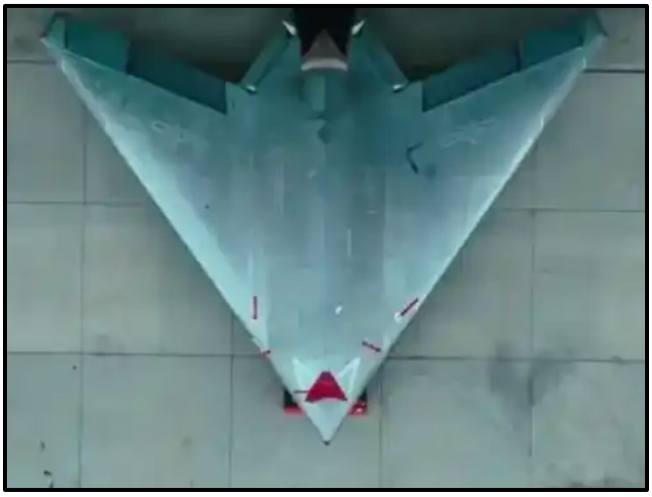
- **PLA Purges:** New indicators suggest that CCP General Secretary Xi Jinping launched investigations into two of the seniormost PLA officers because he perceived them as undermining his leadership and military modernization objectives.
- **CCP engagement with Taiwan:** The CCP held an exchange with the main Taiwanese opposition party, KMT, for the first time since 2016. This exchange may facilitate CCP efforts to co-opt KMT elements as a vector for influencing Taiwanese politics.
- **Adiz Incursions:** PLA sorties into Taiwan's Air Defense Identification Zone (ADIZ) in January 2026 declined to their lowest monthly volume since before President Lai's inauguration.



MILITARYWATCH: CHINA'S NEW UNMANNED LONG RANGE STEALTH FIGHTER NOW BEING TESTED ON CARRIER DECKS

New footage has confirmed that the new Chinese aircraft carrier *Sichuan* has begun testing the integration of an unmanned long range stealth fighter thought to be from the GJ-11 series. The aircraft appeared on the *Sichuan's* lift, and subsequently on its deck, hours before the carrier went out to sea for its second set of sea trials. The possibility remains that what was seen was a full-scale mockup used to practice flight deck management, rather than an actual aircraft. The *Sichuan*, a Type 076 class carrier, is one of just three carrier types in the world integrating an electromagnetic catapult launch system (EMALS), and for close to half a decade before its launch in December 2024 it has been expected to serve as a carrier for unmanned fixed wing aircraft, in particular long range flying wing designs like the GJ-11. In parallel to ongoing work to operationalize a naval variant of the aircraft, a land-based variant of the GJ-11 began its first known deployment in the Air Force in October 2025.

Although the Chinese People's Liberation Army Navy's J-35 fifth generation fighter is the only stealth aircraft in the world integrated with a carrier EMALS, and alongside the American F-35B/C is the only carrier-based stealth fighter operational worldwide, this is expected to change once the *Sichuan* and its air wing enter service. The *Sichuan* began its first sea trails on 14 November 2025, and displaces 50,000 tons, making it larger than the significant majority of carriers in the world. The ship blurs the line between an amphibious assault ship, like the lighter Type 075 class on which its design is based, and a full aircraft carrier. The design has no direct analogues with similar displacements or capabilities anywhere in the world and has the potential to be particularly revolutionary for Chinese carrier aviation.



Although flying wing aircraft like the GJ-11 are not well suited to achieving high levels of speed or maneuverability, their designs are optimal for high-altitude long-range operations and for retaining high degrees of stealth. The American B-2 Spirit bomber program, which first flew in the late 1980s, played a pioneering role in operationalizing these designs, despite the program having itself been far from successful. GJ-11 squadrons deployed from carriers could provide a highly potent offensive capability, with their ability to take off from ships far out at sea, combined with their advanced stealth capabilities and long ranges, expected to make strikes and the directions from which they will be launched difficult to predict. The GJ-11 is one of several unmanned stealth fighters confirmed to be under development in China, with work currently ongoing on more ambitious programs to develop more maneuverable aircraft with higher levels of autonomy, such as the Dark Sword fighter. It is expected that the benefits of fielding unmanned stealth aircraft like the GJ-11, and advances in artificial intelligence and in data links making their operations more effective, will increase interest from multiple carrier-operating countries in fielding a similar capability to that currently being pioneered onboard the *Sichuan*.

ARMYRECOGNITION: BANGLADESH SIGNS CHINA DEAL TO LOCALLY PRODUCE MILITARY AERIAL DRONES WITH FULL TECH TRANSFER

Bangladesh and China have entered into a significant defense agreement that will see the establishment of a drone manufacturing and assembly plant within Bangladesh. The deal, signed between the Bangladesh Air Force and China Electronics Technology Group Corporation International (CETC), includes a full technology transfer, aiming to build local industrial capacity and foster long-term self-reliance in UAV production for Bangladesh. The signing ceremony took place at the BAF headquarters in Dhaka, attended by high-ranking officials from both nations, including the BAF Chief and the Chinese Ambassador.

This landmark project will initially enable Bangladesh to produce and assemble several types of unmanned aerial vehicles, specifically Medium-Altitude Long-Endurance (MALE) and Vertical Take-off and Landing (VTOL) drones. The agreement is not limited to assembly but also encompasses capacity building, joint technical cooperation, and the development of a skilled aerospace workforce through specialized training and knowledge exchange. This initiative is a major step in Bangladesh's broader "Forces Goal 2030" military modernization program.

The UAVs produced are intended for a dual-use role, serving not only in military operations but also in humanitarian assistance and disaster management efforts. By developing its own UAV platforms, the Bangladesh Air Force aims to meet both national and international demand for drones, marking a new era in the nation's defense and technological landscape. This collaboration is expected to significantly contribute to Bangladesh's technological advancement and strategic autonomy in the aerospace sector.

MILITARYWATCH: CHINA'S HEAVILY ENHANCED NEW '5+ GENERATION' J-20A FIGHTER SHOWN IN LANDMARK TESTING

Footage released by the primary developer of the J-20 fifth generation fighter, the Chengdu Aircraft Industry Group, and for the first time shown several of the new and heavily enhanced J-20A variants undergoing test flights in January 2026. The firm announced that the aircraft has successfully completed the systematic test flight organization and training of ten types of aircraft across five locations, which and specifically noted that this included manned and unmanned operations, which are expected to be one of the new defining features of the J-20A. Tests occurred at both indoor and outdoor test sites, while the aircraft were confirmed to have also completed research and development and acceptance test flights.

Although the designation J-20A was previously widely used by analysts to refer to J-20 fighters brought into service from 2021, and integrating the indigenous WS-10C engines, these aircraft have since been confirmed to use the baseline 'J-20' designation, much like the original 40 production models produced in the 2010s which used inferior Russian-supplied stopgap engines. The J-20A instead refers to a new variant with a revised airframe design, with the most conspicuous difference being its redesigned rear canopy which reduces aerodynamic drag, enhances its efficiency in supersonic flight, and is likely to further improve stealth capabilities. The new variant integrates the WS-15 next generation engine, with the first footage of a serial production fighter with the new powerplant having been published in late December 2025.

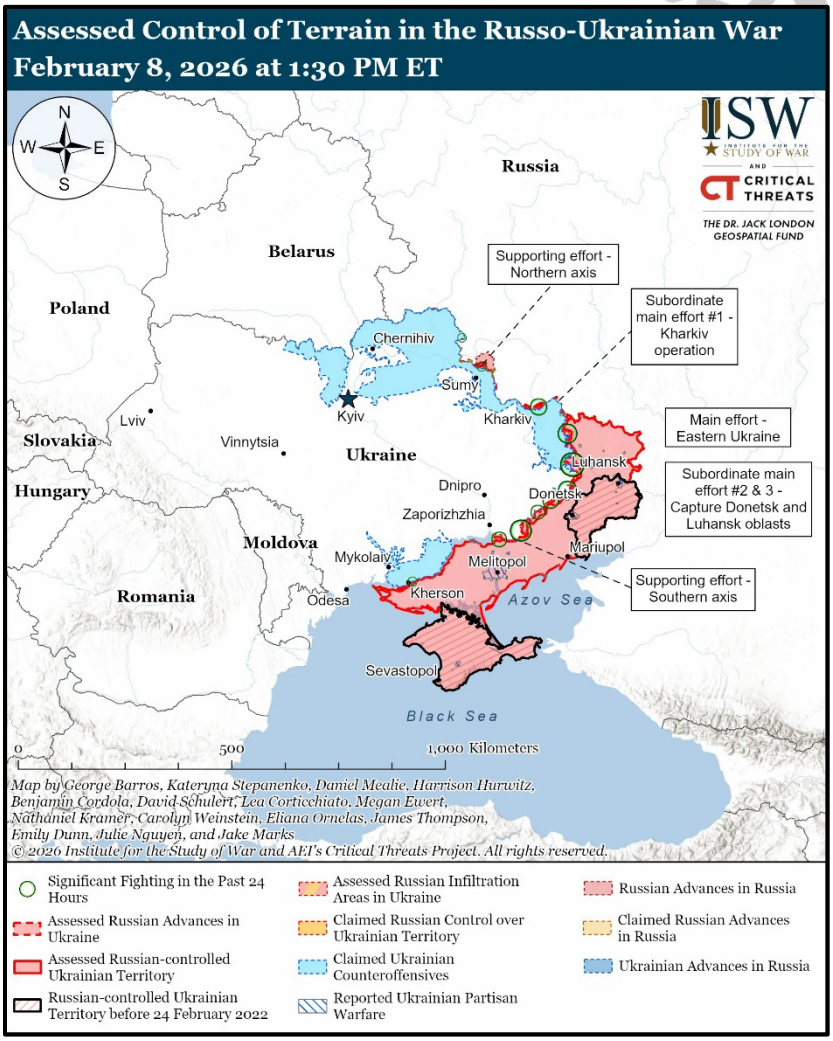
The integration of the WS-15 has long been anticipated, with the engine first seen integrated onto the J-20 in single configuration for a test flight in January 2022, before it was subsequently first flown in twin configuration in June 2023. It significantly improves all aspects of the J-20's flight performance, as well as its range, while providing greater power to onboard subsystems and reducing maintenance requirements. With its capabilities improving significantly, the J-20 is being brought into service by the Chinese People's Liberation Army Air Force much more rapidly than any other fighter type by any other service in the world, with the Air Force expected to field approximately 1000 of the aircraft by 2030. Despite the J-20's increasingly advanced capabilities and central role in China's defense, the development of three separate sixth generation long range fighter types, the first of which is scheduled to enter service in the early 2030s, has raised questions regarding the future of the fifth generation program and whether the aircraft may be phased out of production in little over half a decade.

EUCOM

ISW: RUSSIA-UKRAINE UPDATE

Key Takeaways:

- **Cognitive Warfare**: Russian forces are continuing their cognitive warfare campaign that uses small-scale cross-border attacks in previously dormant frontline areas in northern Ukraine to try to convince the West that the frontlines in Ukraine are collapsing.
- **Starlink Blockage**: Russian milbloggers continue to claim that SpaceX's recent block of unregistered Starlink terminals in Ukraine is hindering Russian combat operations in Ukraine.
- **Drone Warfare**: Russian forces continue to integrate air-to-air capabilities onto their Shahed-type drones to ensure the drones evade Ukrainian air defenders and to undermine Ukraine's air defense.
- Parts of Ukraine's defense industrial base (DIB) have achieved self-sufficiency such that Ukraine can start exports to the West.
- The Ukrainian General Staff confirmed that Ukrainian missile strikes in January 2026 damaged parts of Russia's Kapustin Yar launch site.
- Ukrainian forces recently advanced near Hulyaipole.



APNEWS: RUSSIA BOMBARDS UKRAINE WITH DRONES AND MISSILES A DAY BEFORE PLANNED PEACE TALKS

Russia carried out a major overnight attack on Ukraine in what President Volodymyr Zelenskyy said Tuesday was a broken commitment to halt striking energy infrastructure as the countries prepared for more talks on ending Moscow's 4-year-old full-scale invasion. The bombardment included hundreds of drones and a record 32 ballistic missiles, wounding at least 10 people. It specifically took aim at the power grid, Zelenskyy said, as part of what Ukraine says is Moscow's ongoing campaign to deny civilians light, heating and running water during the coldest winter in years. "Taking advantage of the coldest days of winter to terrorize people is more important to Russia than diplomacy," Zelenskyy said. Temperatures in Kyiv fell to minus 20 degrees Celsius (minus 4 Fahrenheit) during the night and stood at minus 16 C (minus 3 F) on Tuesday.

A Kremlin official said last week that Russia had agreed to halt strikes on Kyiv for a week until 1 February because of the frigid temperatures, following a personal request from U.S. President Donald Trump to Russian President Vladimir Putin. However, the bitter cold is continuing and so are Russia's aerial attacks. Zelenskyy, however, accused Russia of breaking its commitment to hold off its attacks on Ukraine's energy assets, claiming the weeklong pause was due to come into force last Friday. "We believe this Russian strike clearly violates what the American side discussed, and there must be consequences," he said. The bombardment of at least five regions of Ukraine comprised 450 long-range drones and 70 missiles, Ukrainian officials said. Russian officials provided no immediate response to Zelenskyy's comments.

In Kyiv, officials said that five people were wounded in the strikes that damaged and set fire to residential buildings, a kindergarten and a gas station in various parts of the capital, according to the State Emergency Service. By early morning, 1,170 apartment buildings in the capital were without heating, Kyiv Mayor Vitali Klitschko said. That set back desperate repair operations that had restored heat to all but 80 apartment buildings before the attack, he said. Russia also struck Ukraine's northeastern Kharkiv region, where injuries were reported, and the southern Odesa region. The attack also damaged the Hall of Fame at the National Museum of the History of Ukraine in the Second World War, in Kyiv, Ukrainian Culture Minister Tetiana Berezhna said.

DEFENSENEWS: POLAND PICKS KONGSBERG-PGZ CONSORTIUM TO BUILD ANTI-DRONE 'WALL'

Poland's Ministry of National Defence has signed a deal with a consortium comprising Norway's Kongsberg Defence & Aerospace and Polish state-run defense group PGZ to acquire counter-unmanned aerial systems (CUAS) that will protect the country's airspace. The purchase comes in response to incursions by Russian drones that Moscow has perpetrated against Poland alongside Russia's ongoing invasion of Ukraine. Signed on 30 January in the presence of Polish Prime Minister Donald Tusk and Władysław Kosiniak-Kamysz, who is deputy prime minister and defense minister, the deal paves the way for the development of the San anti-drone system whose value is estimated at around PLN 15 billion ($4.2 billion). In his remarks, the deputy prime minister referred to last September's violations of Polish airspace by Russian unmanned aerial vehicles (UAVs). The drone threats had triggered action by the Polish and allied air forces which included scrambling F-35 fighter jets to shoot the the drones down. "The night of 9-10 September 2025, when our airspace was violated, when Russian unmanned aerial vehicles first appeared over NATO territory, was a turning point," Kosiniak-Kamysz said. "It was a moment when we all wondered what else could be done. Research on this equipment took many months: integration, combining all the elements into one well-functioning system."

The value of Kongsberg's share of the deal is around NOK 16 billion ($1.66 billion). In a statement, the Norwegian company said the batteries that are to be supplied to Poland's military will comprise a wide range of effectors, including 35mm, 30mm and 12.7mm guns, as well as missiles, interceptor drones and other solutions. The system is based on Kongsberg's Protector family of weapons, including the Medium Caliber Turret (MCT30) and the Remote Weapon Station, the producer said in a statement. The acquisition "confirms Poland's position as a regional hub for counter-drone innovation and strengthens Kongsberg's positions as one of Europe's leading providers of anti-drone solutions," said Eirik Lie, the president of Kongsberg Defence & Aerospace.
The prime minister said that, in the aftermath of Russia's attack against Ukraine, Poland seeks to strengthen its military cooperation with the Baltic States and Scandinavian countries. "Deliveries of the entire system are expected to be completed 24 months following the signing of the contract," PGZ said.

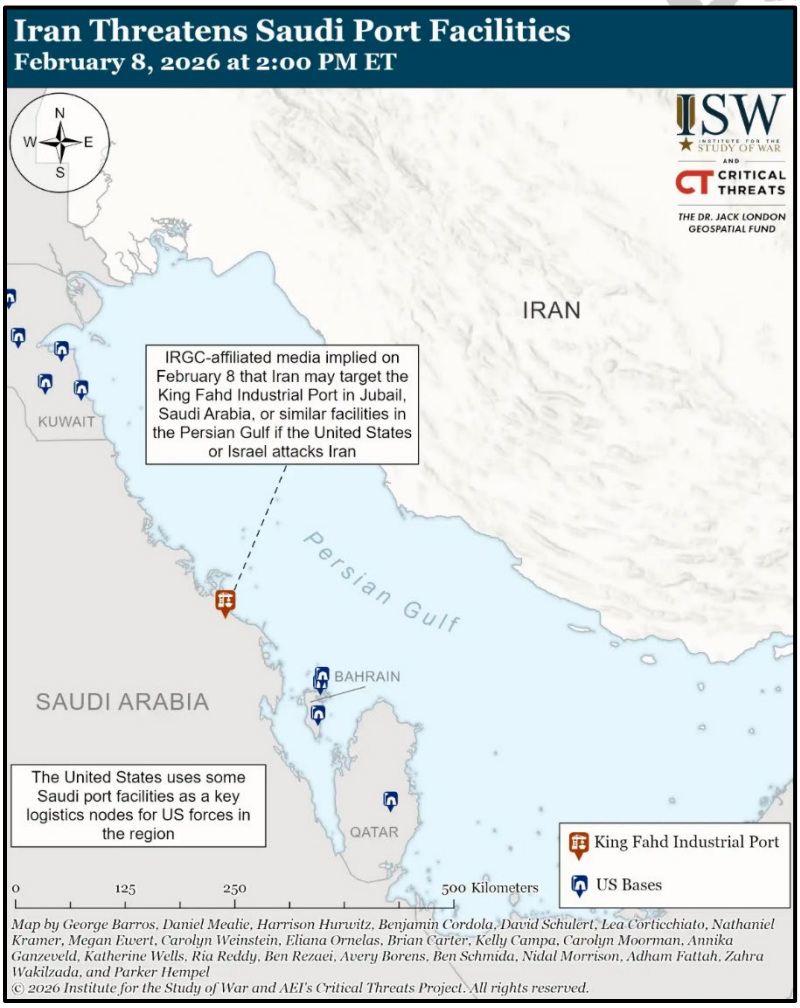
The SAN program represents a key initiative to boost Poland's air-defense capabilities. The Polish ministry has also ordered Common Anti-air Modular Missiles, or CAMM, as well as iLaunchers from European consortium MBDA. The weapons are part of the nation's Narew short-range air defense system developed by PGZ. The ministry has also purchased Pilica+ very-short-range air defense batteries from the Polish defense industry. The Narew and Pilica+ systems will complement the two Patriot Configuration 3+ batteries Poland purchased in 2018 under the Wisła mid-range air defense program, and the second phase of the program announced in May 2022 under which the country seeks a further six batteries of the system made by Raytheon. Kosiniak-Kamysz said that, in total, Warsaw intends to spend around PLN 250 billion on bolstering its air defense capabilities which could make the effort the largest acquisition program for the Polish military in history. "We are building another layer of the air defense system. We have the Wisła, we have the Narew, we have the Pilica, and we are now adding the San," he said.

CENTCOM

ISW: CENTCOM UPDATE

Key Takeaways:

- **U.S.-Israel Talks:** U.S. President Donald Trump and Israeli Prime Minister Benjamin Netanyahu will meet in Washington D.C, on 11 February to discuss Iran. Israeli officials have consistently said that U.S.-Iran negotiations must include limitations on Iran's ballistic missile program.
- **U.S.-Iran Negotiations:** Iran has not changed its negotiating position, which makes a diplomatic breakthrough in future talks unlikely unless the United States alters its negotiating position.
- **A Potential Iranian Retaliatory Attack:** Islamic Revolutionary Guard Corps (IRGC)-affiliated Fars News reported on 8 February that Iran may target supply centers and ports in the region if the United States or Israel attacks Iran.
- **U.S.-Saudi Naval Cooperation:** The Saudi Defense Ministry announced on 7 February that the United States and Saudi Arabia conducted a joint naval exercise at the King Faisal Naval Base in Jeddah.



ARMYRECOGNITION: IRAN'S ARMY FIELDS 1,000 NEWLY DEVELOPED DRONES AMID ESCALATING U.S. PRESSURE

Iran's regular army has formally integrated 1,000 newly developed unmanned aerial systems into the combat organization of its service branches, Iranian state media reported on 29 January 2026. Iranian reporting states the drones were produced through cooperation between army specialists and the Ministry of Defense, implying a procurement model closely tied to field requirements. While Tehran does not publish the exact models or allocations, the emphasis on multi-domain employment suggests the drones are intended to support not only tactical battlefield tasks but also broader deterrence planning, particularly in sensitive maritime corridors. Several Iranian drone families provide a realistic technical baseline for what this kind of integration can deliver. The Shahed-136 loitering munition, widely documented in open sources, is generally assessed with a range in the 540–1,350 NM class depending on payload and flight profile, and is designed for low-cost saturation attacks against fixed infrastructure targets. A smaller companion design, the Shahed-131, follows the same logic in a more compact airframe, allowing higher numbers to be fielded and launched from dispersed locations.

Systems in the Mohajer family, including the Mohajer-6, are commonly associated with electro-optical and infrared (EO/IR) sensor payloads and are often cited with endurance around 12 hours and line-of-sight datalink ranges around 108 NMs. Such drones enable persistent observation, target confirmation, and rapid cueing of fires, especially when paired with artillery, rockets, or loitering munitions already positioned in depth. The operational advantage lies less in a single drone's sophistication than in the ability to maintain continuous coverage over multiple sectors. From a tactical and operational perspective, integrating 1,000 drones enables Iran to build redundancy and persistence into its planning. Reconnaissance drones expand the surveillance envelope and reduce uncertainty around target movement. Attritable loitering munitions provide volume, allowing saturation of point defenses and increasing the probability of penetration. The same mass complicates interception economics, since low-cost drones can force defenders to expend high-value interceptors or reveal air defense positions. Maritime tasking further amplifies the effect, as drones can support coastal surveillance, track surface traffic, and cue shore-based anti-ship fires, tightening Iran's control over escalation ladders around chokepoints.

The integration also takes place amid heightened Iran–U.S. tension. In this context, mass drone induction serves both military readiness and strategic messaging: it communicates that Iran's retaliatory options are distributed, scalable, and difficult to preempt. For regional and international security, the core implication is the accelerating normalization of large-scale unmanned warfare. Iran's model favors numbers, dispersal, and attrition tolerance, which shifts the burden onto defenders to invest in layered counter-UAS architectures, rapid-reaction interceptors, electronic protection, and resilient command networks. As more actors adopt similar approaches, crisis stability deteriorates warning times shrink, attribution can become harder, and escalation can move faster than diplomatic control. In the Gulf and beyond, the result is a defense environment increasingly shaped by persistence, saturation, and electronic contest, rather than by a narrow competition in manned platforms alone

DEFENSENEWS: RUSSIA TO SHOWCASE NEW MLRS AT SAUDI WEAPONS SHOW, SEEKING LOCAL TIES

Russia will unveil its newest multiple launch rocket system, the Sarma, at the World Defense Show 2026 in Riyadh next month, marking Moscow's latest effort to court Middle Eastern defense customers despite Western sanctions targeting its defense industry. The 300mm Sarma MLRS, mounted on a KAMAZ-63501 8x8 armored chassis, represents Russia's attempt to field a lighter, more mobile alternative to its existing heavy rocket artillery systems, state tech corporation Rostec announced Jan. 30. The system features six launch tubes, a reduced configuration compared to the 12-tube Tornado-S and BM-30 Smerch systems currently in Russian service, according to imagery shown on Russian television.

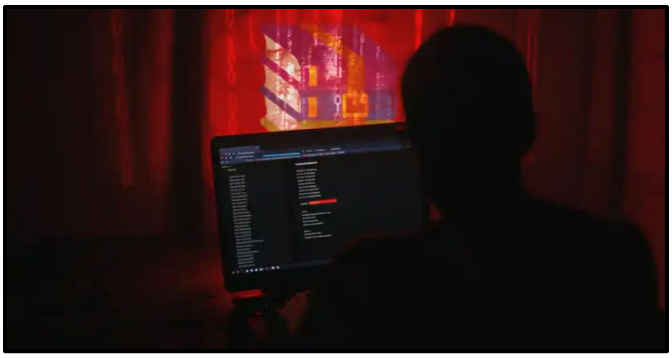
Russia moved the Sarma from prototype to procurement in late 2025, ordering two divisions comprising 12 launchers and 12 transport loading vehicles at a total cost of approximately 2.6 billion Rubles ($35 million), according to contract data reported by Ukrainian defense publication Militarnyi. Moscow needs to deploy more survivable artillery systems on a battlefield increasingly dominated by counter-battery radars and loitering munitions. The Sarma's three-person crew can conduct all operations from within the armored cabin, which Rostec says protects against shrapnel and armor-piercing incendiary ammunition. The system can also be operated remotely from a shelter, addressing Russian concerns about crew vulnerability to drone attacks and precision strikes. Russian sources claim the system can fire guided rockets to ranges approaching 108 NMs. Crew survivability has become a key concern on the battlefield in Ukraine, which is swarming with explosive-laden drones seeking out foot soldiers.

The decision to premiere the system in Riyadh underscores Rosoboronexport's continued interest in Middle Eastern markets, where regional militaries often prioritize hardy and relatively cheap systems capable of operating in rough conditions, and authoritarian governments are more agnostic toward great power politics. By showcasing a lighter 300mm platform alongside more established systems, Russia is positioning itself as an alternative to Western and Asian competitors in a market segment that includes the U.S.-made HIMARS and similar precision rocket artillery. While Rosoboronexport remains subject to extensive U.S. and European sanctions targeting Russia's defense industry and financial sector, no United Nations embargo restricts Russian conventional arms exports, and several Middle Eastern states do not apply Western sanctions regimes or have the same moral qualms about striking a deal with Moscow. Russia's exhibition will also include the BTR-22 8x8 armored vehicle, the Ballista remote weapon station, and the Planshet-A fire control system, according to Russian state media.

CYBERCOM

THEHACKERNEWS: CHINA-LINKED AMARANTH-DRAGON EXPLOITS WINRAR FLAW IN ESPIONAGE CAMPAIGNS

Threat actors affiliated with China have been attributed to a fresh set of cyber espionage campaigns targeting government and law enforcement agencies across Southeast Asia throughout 2025. Check Point Research is tracking the previously undocumented activity cluster under the moniker Amaranth-Dragon, which it said shares links to the APT 41 ecosystem. Targeted countries include Cambodia, Thailand, Laos, Indonesia, Singapore, and the Philippines. The most notable aspect of threat actors' tradecraft is the high degree of stealth, with the campaigns "highly controlled" and the attack infrastructure configured such that it can interact only with victims in specific target countries in an attempt to minimize exposure. Attack chains mounted by the adversary have been found to abuse CVE-2025-8088, a now-patched security flaw impacting RARLAB WinRAR that allows for arbitrary code execution when specially crafted archives are opened by targets.



Although the exact initial access vector remains unknown at this stage, the highly targeted nature of the campaigns, coupled with the use of tailored lures related to political, economic, or military developments in the region, suggests the use of spear-phishing emails to distribute the archive files hosted on well-known cloud platforms like Dropbox to lower suspicion and bypass traditional perimeter defenses. The archive contains several files, including a malicious DLL named Amaranth Loader that's launched by means of DLL side-loading, another long-preferred tactic among Chinese threat actors. The loader shares similarities with tools such as DodgeBox, DUSTPAN (aka StealthVector), and DUSTTRAP, which have been previously identified as used by the APT41 hacking crew

Once executed, the loader is designed to contact an external server to retrieve an encryption key, which is then used to decrypt an encrypted payload retrieved from a different URL and execute it directly in memory. The final payload deployed as part of the attack is the open-source command-and-control (C2 or C&C) framework known as Havoc.

In contrast, early iterations of the campaign detected in March 2025 made use of ZIP files containing Windows shortcuts (LNK) and batch (BAT) to decrypt and execute the Amaranth Loader using DLL side-loading. In another campaign targeting Indonesia in early September 2025, the threat actors opted to distribute a password-protected RAR archive from Dropbox so as to deliver a fully functional remote access trojan (RAT) codenamed TGAmaranth RAT instead of Amaranth Loader that leverages a hard-coded Telegram bot for C2 What's more, the C2 infrastructure is secured by Cloudflare and is configured to accept traffic only from IP addresses within the specific country or countries targeted in each operation. The activity also exemplifies how sophisticated threat actors weaponize legitimate, trusted infrastructure to execute targeted attacks while remaining operational clandestinely.

CYBERSECURITYNEWS: RUSSIAN HACKER ALLIANCE TARGETING DENMARK IN LARGE-SCALE CYBERATTACK

A newly formed Russian hacker alliance known as Russian Legion has launched a coordinated cyberattack campaign against Denmark. The alliance publicly announced its formation on 27 January 2026, marking a significant escalation in state-aligned hacktivist operations targeting Western nations. The group initiated “OpDenmark” with a series of distributed denial-of-service (DDoS) attacks aimed at disrupting Danish organizations and pressuring the government over its military support for Ukraine. The campaign began when Russian Legion issued an ultimatum on 28 January 2026, demanding that Denmark withdraw its planned 1.5 billion DKK military aid package to Ukraine within 48 hours. The group warned that DDoS attacks were only preliminary actions, stating that more severe cyber operations would follow if their demands were ignored. Shortly after the deadline passed, multiple Danish companies and public sector organizations reported service disruptions, with the energy sector experiencing repeated targeting.

Truesec analysts identified the Russian Legion as a state-aligned but not state-funded threat actor, operating independently while supporting Russian geopolitical objectives. The alliance represents a coordinated effort by established hacktivist groups to amplify their operational impact through joint campaigns. The attacks have primarily focused on overwhelming target systems through

DDoS techniques, rendering websites and online services temporarily inaccessible. According to the threat actors' public statements, the main assault was scheduled to commence at 4 PM Danish time, targeting both private enterprises and government infrastructure. Inteid, one of the alliance members, had already conducted preliminary attacks against sundhed.dk earlier in the week, demonstrating the group's capability to disrupt healthcare services.

Russian Legion employs a multi-layered strategy that combines technical disruption with psychological operations. The group leverages DDoS-for-hire services to generate massive traffic volumes, overwhelming target networks and exhausting defensive resources. Their approach begins with public threats broadcast through Telegram channels, followed by low-impact attacks that serve as proof-of-capability demonstrations. The threat actors then post screenshots of affected websites to amplify fear and create media attention, even when actual damage remains limited. This psychological component aims to generate uncertainty among Danish citizens and pressure decision-makers, though historical data suggests these campaigns rarely escalate to catastrophic outcomes when organizations implement proper defensive measures including rate limiting, geo-blocking, and specialized DDoS protection services.

ADDITIONAL RESOURCES

AFMC A2: World Threat Brief CAO: 6 Oct 2025
https://usaf.dps.mil/sites/22244/SitePages/Command-Intel-Threat-Brief.aspx

China Aerospace Studies Institute: CASI supports the Secretary of the Air Force, Joint Chiefs of Staff, and other senior leaders of the Air and Space Forces. CASI provides expert research and analysis supporting decision and policy makers in the Department of Defense and across the U.S. government.
https://www.airuniversity.af.edu/CASI/

The Center for Strategic and International Studies (CSIS): is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.
https://www.csis.org/

Defense Intelligence Agency Military Power Publications: an intelligence agency and combat support agency of the United States Department of Defense, specializing in defense and military intelligence.
https://www.dia.mil/Military-Power-Publications/

Institute for the Study of War: The Institute for the Study of War (ISW) is a non-partisan, non-profit, public policy research organization. ISW advances an informed understanding of military affairs through reliable research, trusted analysis, and innovative education.
https://www.understandingwar.org/

Perun: An Australian covering the military industrial complex and national military investment strategy.
https://www.youtube.com/@PerunAU

Research and Development Corporation (RAND): RAND is a nonprofit, nonpartisan research organization that provides leaders with the information they need to make evidence-based decisions.
https://www.rand.org/

RealClearDefense: RCD was created at the request of the Pentagon and Hill staff on the House Armed Services Committee for information about military affairs, defense policy, national security, and foreign affairs.
https://www.realcleardefense.com/

Stockholm International Peace Research Institute: SIPRI is an independent international institute providing data, analysis and recommendations, based on open sources, to policymakers, researchers, media and the interested public.
https://www.sipri.org/

Task & Purpose: Task & Purpose aims to inform, engage, entertain, and stand up for active-duty military members, veterans, and their families. The site quickly became one of the most trusted news and investigative journalism sources for the military, with its journalists reporting everywhere from the Pentagon to The White House and beyond.
https://www.youtube.com/@Taskandpurpose

FRONTLINE examines the rise of Xi Jinping, his vision for China and the global implications. Correspondent Martin Smith traces the defining moments for President Xi, how he's exercising power and his impact on China, and relations with the U.S. and the world.
https://www.pbs.org/wgbh/frontline/documentary/china-the-u-s-the-rise-of-xi-jinping/