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

March 23, 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

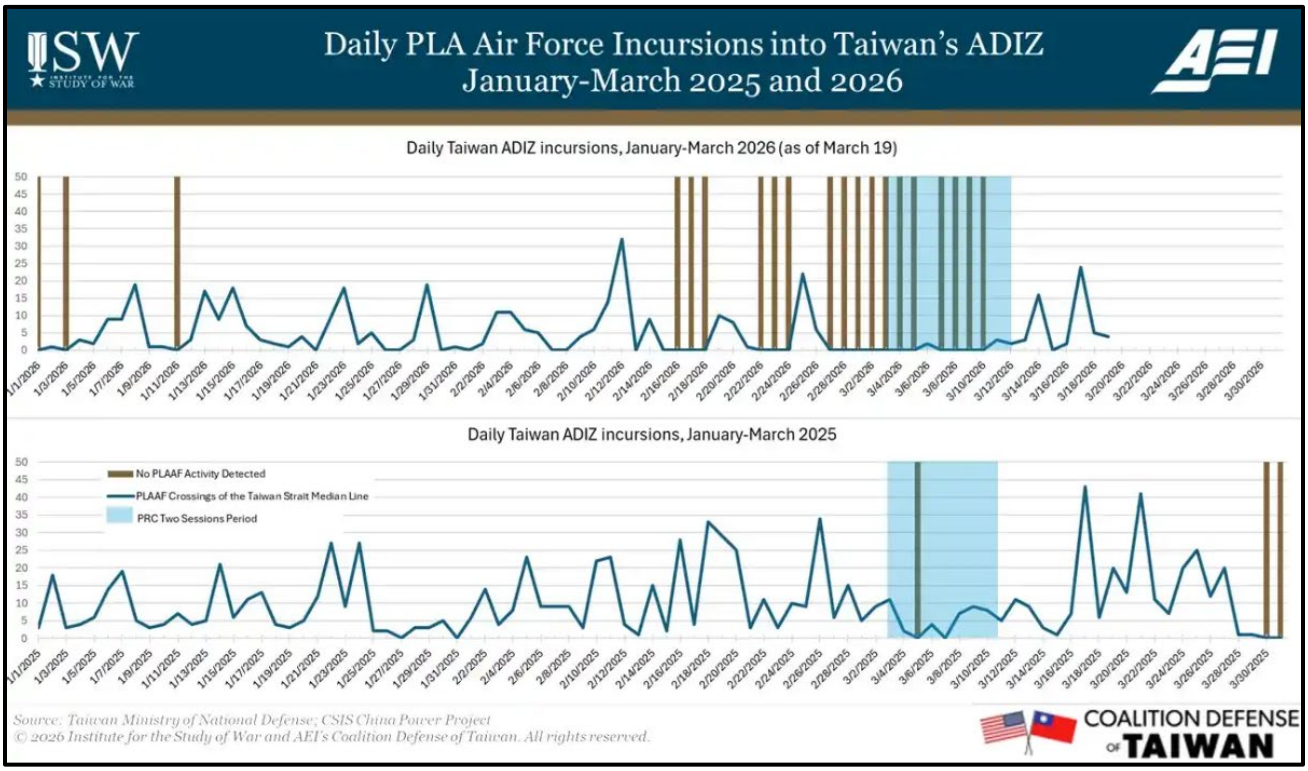
We value your thoughts on the Gryphon Growl—share them with us!
Your input helps improve and enhance our product.

INDOPACOM

ISW: CHINA-TAIWAN UPDATE

Key Takeaways:

- **U.S.-PRC meetings:** U.S. President Donald Trump announced on 17 March that he would delay his planned talks with CCP General Secretary Xi Jinping to prioritize the conflict in Iran.
- **PRC narrative warfare:** Taiwanese think tank Doublethink Lab published a report revealing that a PRC state-affiliated firm compiled information on tens of thousands of prominent Taiwanese people, including 170 politicians, to support PRC cognitive warfare and election interference campaigns in Taiwan.



MILITARYWATCH: WORLD'S LONGEST RANGE ROCKET ARTILLERY SYSTEM DEMONSTRATES AI-POWERED DEEP STRIKE CAPABILITIES IN NORTH KOREAN LIVE FIRE DRILL

The Korean People's Army recently held a firepower strike drill using its unique KN-25 600-millimeter rocket artillery system, firing twelve rockets described as having "ultra-precision" capabilities. The exercise, which took place on 14 March, was reported by the Korean Central News Agency (KCNA) and was observed hours earlier by South Korea, who initially identified the launches as approximately 10 ballistic missiles. This drill is widely seen as a direct response to the ongoing joint military exercises between the United States and South Korea and served to demonstrate the capabilities of new KN-25 system variants.

Supervising the launch, North Korean leader Kim Jong-un stated that the KN-25 systems would be used for a "massive, destructive strike" if deterrence fails to prevent an armed provocation. The timing of this drill is particularly notable, as the United States has reportedly withdrawn its MIM-104 Patriot and THAAD missile defense systems from South Korea, leaving U.S. military bases in the region more vulnerable. This test follows the recent delivery of a large batch of 50 KN-25 launchers to the Korean People's Army in late February, significantly boosting their artillery forces.

The KN-25 is a highly advanced weapons system, with Chairman Kim highlighting that it "perfectly combines the accuracy and destructive power of tactical ballistic missiles with the firing speed of multiple rocket launchers," utilizing AI technology and a combined guidance system. Considered by many analysts to be the world's longest-ranged rocket artillery system with a reported range of 216 nautical miles, it "blurs the line between rocket and missile," according to a U.S. Congressional Research Service report. There have also been unconfirmed reports that the KN-25 has been exported to Russia, with arms sales potentially funding the expansion of North Korea's defense production.

ARMYRECOGNITION: JAPAN DEPLOYS FIRST UPGRADED TYPE 12 LONG-RANGE ANTI-SHIP MISSILES NEAR EAST CHINA SEA

Japan has initiated the deployment of its upgraded Type-12 land-to-ship missiles, with the first operational units arriving at Camp Kengun in Kumamoto Prefecture. This move marks the first practical application of Tokyo's new long-range strike capability, aimed at enhancing its defensive posture along the southwestern island chain. The initial convoy of launch vehicles and support equipment traveled from Camp Fuji, where research units are based, to the Kumamoto garrison. This deployment is a significant step in Japan's effort to strengthen its deterrence in the strategically important East China Sea.

The weapon system at the heart of this deployment is the Type-12 Surface-to-Ship Missile (12SSM), developed by Mitsubishi Heavy Industries. Originally a coastal defense missile with a range of about 200 kilometers, the upgraded "Extended Range" variant can now strike targets over 540 nautical miles away. This significant increase in reach is achieved through a redesigned airframe with a reduced radar signature, an improved turbofan engine, and an advanced guidance system combining satellite, inertial, and terrain-referencing navigation. The missiles are fired from highly mobile 8x8 wheeled transporters, a key feature that allows units to rapidly fire and relocate, thereby increasing their survivability against counterattacks.

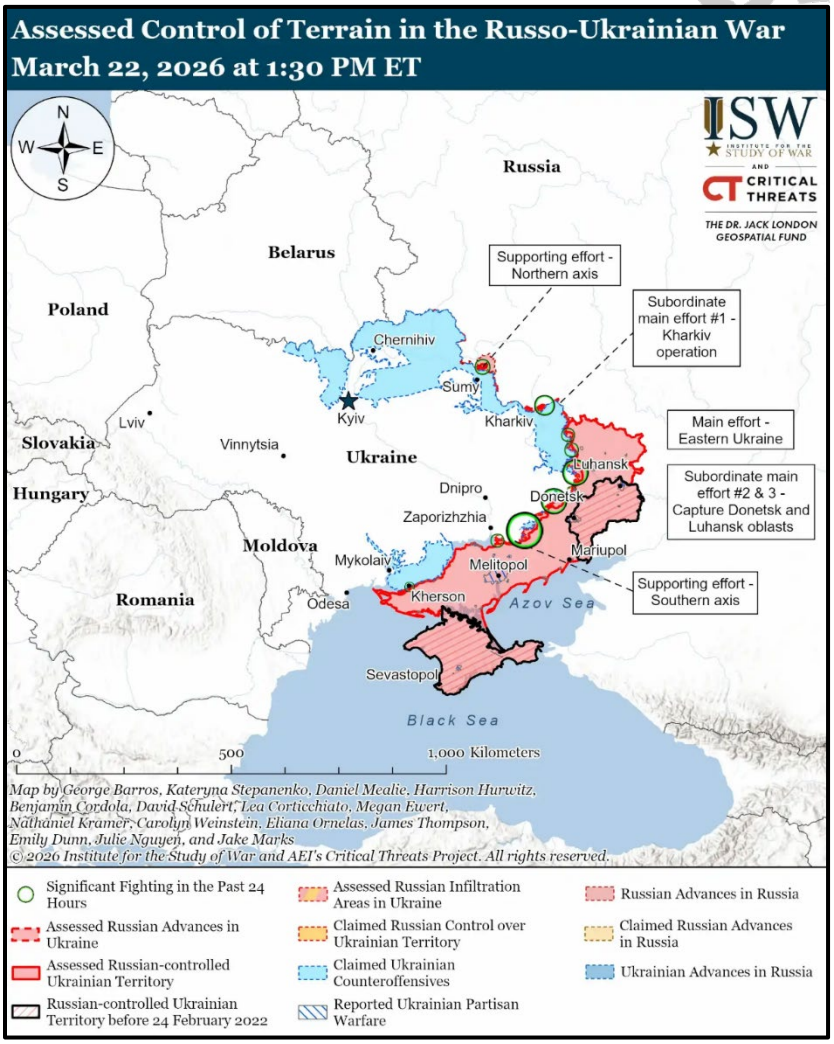
This deployment represents a tangible shift in Japan's national security policy. In late 2022, Tokyo formally adopted a "counterstrike capability," authorizing the acquisition of weapons that can strike enemy bases if Japan is attacked. The placement of these long-range missiles at Camp Kengun is the first implementation of this new, more proactive defense posture. The decision reflects growing regional tensions, particularly increased Chinese military activities around Taiwan and the East China Sea, and positions Japan's southwestern islands as a crucial zone for influencing the regional balance of power with long-range precision weapons.

EUCOM

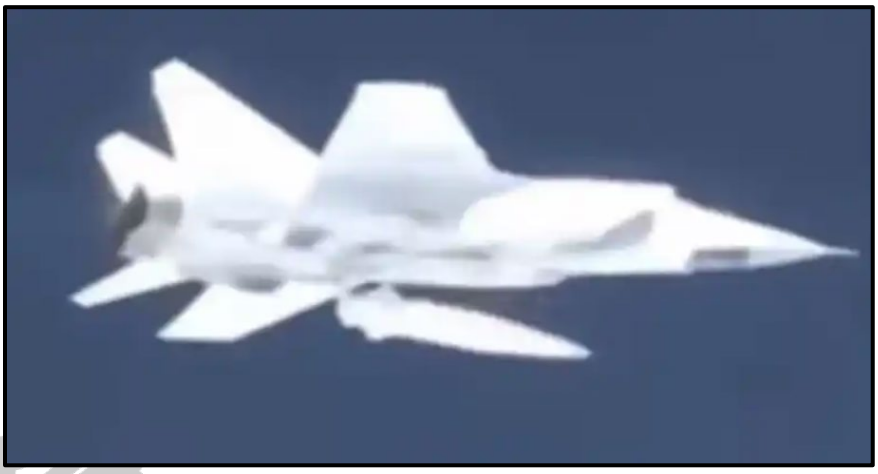
ISW: RUSSIA-UKRAINE UPDATE

Key Takeaways:

- A senior Ukrainian military official forecasted that Russia will begin using mobilized personnel on the battlefield in Ukraine on 1 April.
- Ukrainian counterattacks in southern Ukraine continue to create operational and strategic effects against Russian forces going into the Spring-Summer 2026 offensive.
- Likely Belarusian balloons recently landed in Poland, possibly as part of Russia's ongoing use of Belarus in its "Phase Zero" effort, setting conditions for a potential future war with NATO.
- Ukrainian forces recently advanced in the Kostyantynivka-Druzhkivka tactical area.
- Ukrainian forces struck military assets and oil infrastructure in Russia. Russian forces launched 139 drones against Ukraine.



MILITARYWATCH: RUSSIA CONDUCTS RARE MIG-31I LONG RANGE STRIKE EXERCISES NEAR JAPAN WITH MANEUVERING BALLISTIC MISSILES



The Russian Aerospace Forces have conducted a training exercise over the Sea of Japan, deploying MiG-31I strike aircraft equipped with Kinzhal ballistic missiles. During this exercise, pilots practiced in-flight refueling, a capability that significantly extends the aircraft's operational range and allows them to loiter for extended periods in the strategic maritime corridor between Japan and the Korean Peninsula. The deployment is highlighted as particularly significant due to the withdrawal of U.S. forces and missile defense assets from the region, which has reportedly shifted the local balance of power.

The MiG-31I is a specialized strike variant of the MiG-31, the world's fastest and highest-flying combat aircraft. Its impressive performance, including a sustained cruising speed of Mach 2.35, allows it to impart significant kinetic energy to the Kinzhal missile upon launch. The Kinzhal itself is an air-launched version of the Iskander-M ground-based ballistic missile. While MiG-31 interceptors have been present in the Pacific since the early 1980s, the deployment of variants configured to carry ballistic missiles is a new development for the region.

This weapon system has a proven combat record, including the first credited destruction of a U.S.-made MIM-104 Patriot air defense system in May 2023. By October 2025, Ukrainian and Western officials noted that the missile strikes had become significantly more difficult to intercept. The MiG-31I's recently added in-flight refueling capability has been used in combat to launch strikes from deeper within Russian territory. With Russia expected to increase its fleet of these modernized aircraft, they are seen as a growing challenge to the missile defenses of the Western Bloc and its allies.

THEDEFENSEPOST: UKRAINE FIRM TO ENHANCE ITS DRONES WITH GERMAN SIGNALS INTELLIGENCE TECH

Ukrainian drone manufacturer Pegasus Arms has partnered with the German company Rohde & Schwarz to integrate advanced reconnaissance and electronic support systems into its unmanned aerial vehicles (UAVs). This collaboration will combine Pegasus's combat-tested drone platforms with Rohde & Schwarz's expertise in signals intelligence and radio-frequency sensing. The process will involve joint development and testing to directly embed electronic surveillance payloads into the drones, allowing for the real-time collection and processing of signals data from the air.

With over 1,500 heavy UAVs already delivered to Ukrainian forces for strike and logistics missions, Pegasus Arms aims to significantly expand the capabilities of its platforms. The integration of Rohde & Schwarz technology will enable the drones to perform more complex functions, such as identifying and tracking enemy electronic emitters and other drones. This shifts the role of their UAVs from simple strike, logistics, or mine-laying to include critical missions like threat detection, electronic support, and providing enhanced situational awareness on the battlefield, creating what the company director calls "an unpleasant surprise for the enemy."

The agreement will enhance platforms like the Pegasus Arms 25, a modular drone designed for rapid deployment. This UAV is already equipped with features such as resistance to electronic warfare and an autonomous return-to-base function. Currently used for striking vehicles and fortifications, as well as for logistics, the Pegasus Arms 25 has a payload capacity of 30.9 pounds, an operational range of 10.8 nautical miles, and an endurance of up to 45 minutes. The new systems will build upon this existing foundation to introduce a new layer of intelligence-gathering capability.

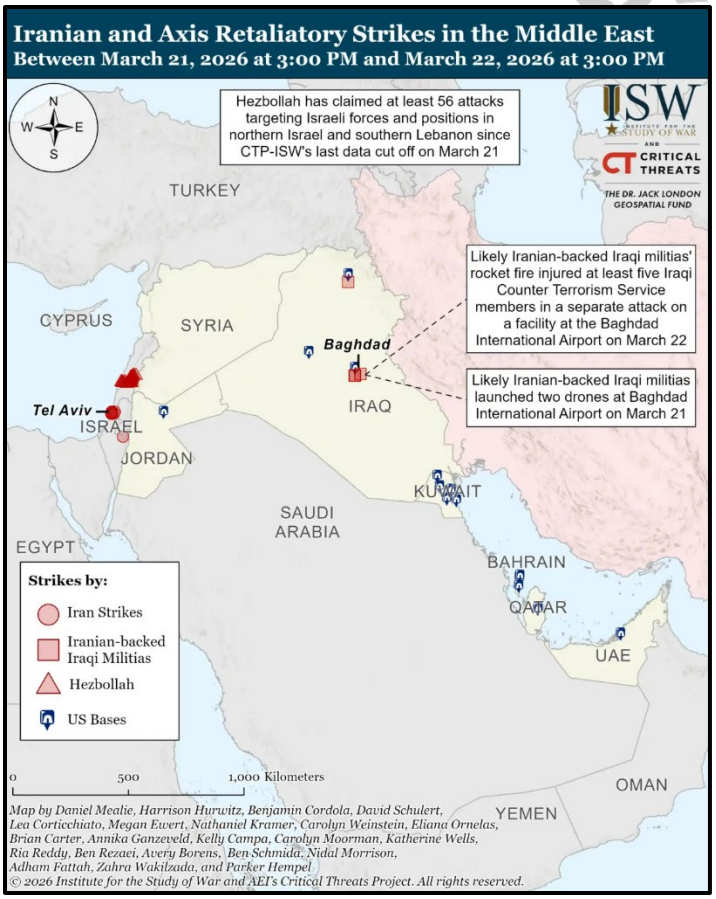
CENTCOM

ISW: CENTCOM UPDATE

Key Takeaways:

- U.S. President Donald Trump threatened on 21 March to “obliterate” Iranian power plants if Iran does not “fully open” the Strait of Hormuz within 48 hours. Iran has threatened to attack regional energy infrastructure if the United States attacks power plants in Iran. ISW-CTP has recorded several Iranian attacks on regional energy infrastructure since the war began on 28 February, but the new threats could entail an expansion of such attacks.

- IRGC Ground Forces Commander Brigadier General Mohammad Karami visited unspecified IRGC Ground Forces units in western and northwestern Iran on 22 March. The visit of the IRGC Ground Forces commander to units in northwestern provinces along Iran’s border is notable given the combined force’s efforts to degrade internal security institutions in Iran’s western border region and reports about possible armed Kurdish mobilization along the Iran-Iraq border.



- The combined force continued to conduct airstrikes targeting Iranian missile production and storage facilities. The combined force targeted sites that produce short- and medium-range ballistic missiles, including the Fath-360 with a maximum range of64.8 nautical miles, Fateh-110 with a maximum range of 162 nautical miles, the Zolfaghar with a maximum range of 378 nautical miles, and the medium-range Haj Qasem ballistic missile with a maximum range of 756 nautical miles. Iran notably has supplied Russia with Fath-360s for Russia’s offensive campaign in Ukraine.

- The IRGC has reportedly restructured Hezbollah under a more decentralized command model following Israeli operations that degraded the group’s leadership in 2024. This decentralized structure aimed to improve operational security and reduce vulnerability to Israeli intelligence penetration.

BREAKINGDEFENSE: GULF NATIONS ‘TRYING TO REACH OUT’ FOR UKRAINIAN COUNTER-DRONE CAPABILITY

As Iranian-made drones successfully penetrate the air defenses of Gulf nations, these governments are turning to Ukraine for its unparalleled expertise in countering such threats. Having contended with swarms of Russian-operated Shahed drones for years, Ukrainian companies have developed unique and effective countermeasures. A communications head for one of Ukraine's largest drone producers, General Cherry, noted that they are receiving a "huge number of requests" from various entities in the Middle East, including private companies and government representatives. This interest represents a crucial financial opportunity for Kyiv, with major deals reportedly in progress with countries like Saudi Arabia, which could provide a much-needed windfall to support Ukraine's ongoing war effort.

Ukraine's success is built upon a "layered" air defense strategy, which emphasizes using low-cost interceptors to destroy inexpensive attack drones. This approach avoids the economically unsustainable practice of using multi-million dollar missiles, like the Patriot, against a $20,000 UAV. The core of this strategy is the interceptor drone, a high-speed FPV (first-person-view) drone designed to physically crash into and neutralize enemy drones. Initially just repurposed FPVs, these interceptors have evolved into specialized systems capable of taking on Shaheds. Ukrainian firms like Wild Hornets, which produces the mass-produced "Sting" interceptor, are already developing next-generation models to counter even faster jet-powered drones.

Despite the high demand and significant production capacity—with President Zelenskyy suggesting 30,000 units could be available for export monthly—a significant hurdle remains. The Ukrainian government maintains strict export controls on domestically produced weapons, meaning manufacturers must direct all interested foreign parties to negotiate with government agencies to get the necessary permissions. This creates a time-sensitive situation, as experts caution that this "unique window of opportunity" will not last. Competitors, including the United States, are already entering the market with their own interceptor drones, and there is a risk that even Russian arms dealers could fill the demand if Ukraine is unable to finalize export deals
.

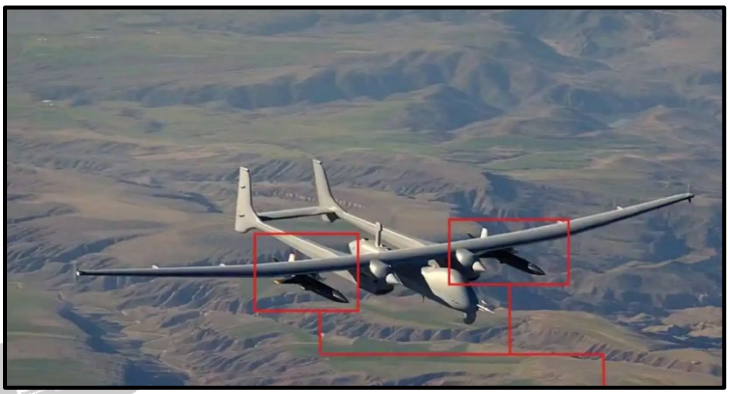
THEDEFENSEPOST: UK MULLS SENDING MINEHUNTER DRONES TO STRAIT OF HORMUZ

The United Kingdom is exploring the deployment of unmanned minehunting systems as a potential contribution to an international effort to reopen the Strait of Hormuz, a critical chokepoint for global oil supplies. British Energy Secretary Ed Miliband confirmed that the government is coordinating with allies, including the United States, to address the disruption. This consideration follows a call from U.S. President Donald Trump for partner nations to send naval assets to secure the shipping lane. Miliband emphasized that all options that could help restore passage are being considered, specifically mentioning mine-hunting drones as one possible contribution.

The potential threat of underwater mines could halt all commercial shipping through the narrow strait, through which approximately 20 percent of the world's oil supply passes. The current tensions have already led to a sharp increase in oil prices. However, there is uncertainty among allies regarding the immediate threat, with the British Defence Secretary stating it was becoming "clearer and clearer" that mines were being laid, while his U.S. counterpart said there was "no clear evidence" of such activity. Furthermore, while unmanned minehunters can reduce risks to crews, analysts have pointed out their operational limitations, including short battery life and the vulnerability of operating within range of Iranian anti-ship missiles.

Despite the potential military contribution, the UK government is stressing a diplomatic and multilateral approach aimed at de-escalation. Prime Minister Keir Starmer stated that his government is working carefully with all partners to create a viable, collective plan that restores freedom of navigation as quickly as possible. He reiterated that the UK will not be drawn into a wider conflict and will continue working towards a resolution that brings security and stability back to the region.

ARMYRECOGNITION: TÜRKIYE FIELDS NEW SÜPER ŞİMŞEK DRONES TO BOOST MULTI-ROLE AIR COMBAT AND STRIKE CAPABILITY



The Turkish Air Force has officially inducted the domestically developed SÜPER ŞİMŞEK, a jet-powered tactical unmanned aerial vehicle (UAV), into its operational inventory. This announcement follows closely after imagery showed a larger AKSUNGUR drone carrying two SÜPER ŞİMŞEK vehicles, signaling a rapid shift from testing to deployment. By bringing this system into service, ürkiye has moved the SÜPER ŞİMŞEK from an experimental project to an operational asset, providing the Air Force with a new indigenous capability for training, deception, force protection, and potential offensive use in contested airspace.

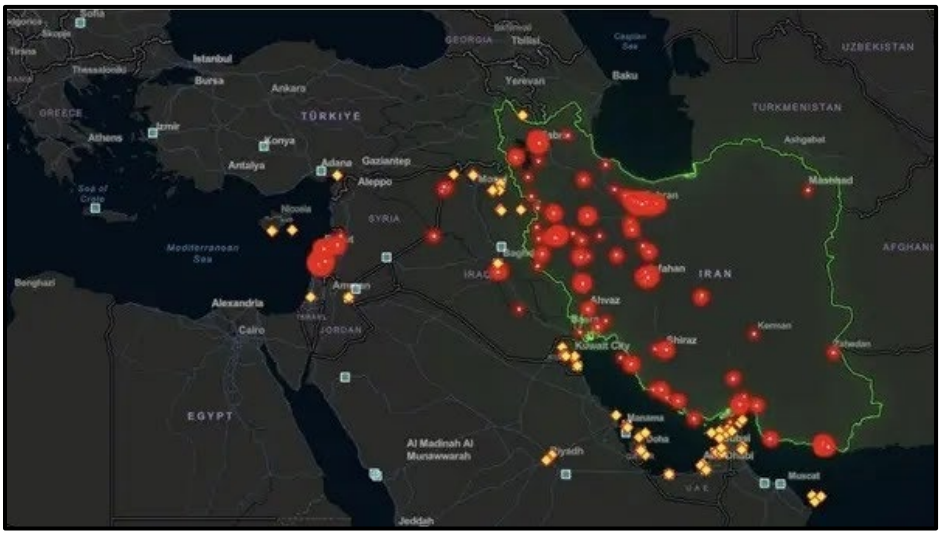
The SÜPER ŞİMŞEK is a versatile platform designed to fill a niche between a target drone, a loitering munition, and a support aircraft. Capable of reaching speeds of Mach 0.85 and an altitude of 35,000 feet, the vehicle has a range of approximately 486 nautical miles. Its key feature is a modular payload architecture that allows it to be configured for various missions. It can be equipped to act as a realistic aerial target, a decoy with an augmented radar or infrared signature, a stand-in electronic jammer, or a one-way attack drone with a 35-kilogram warhead. This adaptability makes it highly valuable for modern air operations, particularly for missions involving the suppression of enemy air defenses (SEAD/DEAD) by saturating and confusing enemy systems.

From a tactical standpoint, SÜPER ŞİMŞEK is an ideal tool for the initial wave of an air campaign, designed to probe and disrupt enemy air defenses to create safe corridors for subsequent strike aircraft. It can be launched from the air by larger drones like the AKSUNGUR and ANKA III, or from the ground using rocket assistance, which provides significant operational flexibility. The induction of this system demonstrates Türkiye's growing capability to build a complete and networked combat aviation ecosystem. For NATO, this development is significant as it strengthens the alliance's southeastern flank with a resilient, domestically produced system that supports the modern doctrine of using lower-cost, expendable unmanned platforms for high-risk missions.

CYBERCOM

CYBERSECURITYNEWS: IRAN-LINKED CYBER CAMPAIGNS CONVERGE WITH ELECTRONIC AND PSYCHOLOGICAL WARFARE AS REGIONAL CONFLICT ESCALATES

Following the start of Operation Epic Fury, Iran and its allies launched a sweeping counter-offensive that fused physical attacks with a highly coordinated cyber warfare campaign. A pre-established network of Iranian-aligned hacktivist groups, directed by the "Islamic Resilience Cyber Axis," mobilized immediately to execute a massive cyber onslaught. This digital assault included widespread distributed denial-of-service (DDoS) attacks, website defacements, and data theft operations aimed at critical infrastructure and government systems across the United States, Israel, and Gulf Cooperation Council nations, demonstrating an intense and immediate digital retaliation.



The cyberattacks were highly specific and damaging, extending beyond simple defacements. The newly emerged Cyber Isnaad Front published a "hit list" of individuals in Israel, while another group, the Handala Hack Team, claimed responsibility for a major cyberattack on the U.S.-based medical technology firm Stryker Corporation, exfiltrating sensitive data as retaliation for a missile strike. Attackers exploited known vulnerabilities in common IoT devices like security cameras to infiltrate networks and targeted critical energy infrastructure. The conflict's digital dimension had physical consequences, with several Amazon data centers in the UAE and Bahrain sustaining damage from drone strikes, compounding the disruption.

Beneath the overt cyberattacks, the conflict featured the most extensive GPS spoofing and jamming campaign ever recorded in a military engagement. Within 24 hours of the initial strikes, Iranian forces and their proxies deployed advanced electronic warfare systems across the Persian Gulf and surrounding airspace, causing widespread navigational chaos. Over 1,700 commercial vessels reported GPS failures in the first week, with their onboard systems being tricked into showing false locations, such as airports or landlocked areas. This "quiet" layer of the war created profound risks for both civilian and military navigation and highlighted the vulnerability of industrial systems that depend on accurate geolocation data.

THEHACKERNEWS: OFAC SANCTIONS DPRK IT WORKER NETWORK FUNDING WMD PROGRAMS THROUGH FAKE REMOTE JOBS

The U.S. Department of the Treasury has sanctioned six individuals and two entities for their roles in a sophisticated North Korean information technology (IT) worker scheme designed to defraud U.S. businesses. These operatives secure remote employment at legitimate companies by using fraudulent documentation, stolen identities, and fabricated personas to hide their true origins. A significant portion of their salaries is then illicitly funneled back to the Democratic People's Republic of Korea (DPRK) to fund its weapons of mass destruction programs, in direct violation of international sanctions. In some instances, these workers also deploy malware to steal sensitive company data, which is then used for extortion.

A key element of this modern fraudulent scheme, known by names like Jasper Sleet and Wagemole, is the extensive use of artificial intelligence. Threat actors leverage AI throughout the attack lifecycle to create convincing digital personas, enhance social engineering efforts, and maintain long-term persistence within target companies. This includes using AI tools like Faceswap to alter identity documents, generating polished resumes, creating fake company websites, and even refining malware components. Operationally, the IT workers often operate from China, using VPN services with U.S. exit nodes to mask their location and appear as legitimate domestic employees, as highlighted in one case where a worker was terminated after their consistent logins from China were detected.

The scheme is supported by a multi-tiered operational structure that includes recruiters, facilitators, IT workers, and collaborators. Recruiters screen candidates, while facilitators and workers create fake personas and secure employment. A crucial part of the operation involves recruiting collaborators, primarily through platforms like LinkedIn and GitHub, who willingly or unwillingly provide their personal information to help the North Korean workers pass hiring processes and receive company-issued equipment. This layered approach allows the operatives to penetrate organizations more deeply and for longer periods, making the scheme a highly integrated and effective component of the DPRK's revenue-generation and sanctions-evasion machinery.

CYBERSECURITYNEWS: IRAN-LINKED BOTNET EXPOSED AFTER OPEN DIRECTORY LEAK REVEALS 15-NODE RELAY NETWORK

A threat actor with ties to Iran has inadvertently exposed their entire botnet infrastructure after carelessly leaving an open directory on a staging server. This critical mistake provided researchers with a rare and detailed view into a live operation, revealing a 15-node relay network, a mass SSH deployment framework, and DDoS tools. The server, hosted by an Iranian ISP, contained 449 files, including deployment scripts, DDoS source code, and a list of credentials used to brute-force access into victim systems, laying bare the group's entire toolkit and methodology.

Analysis of the exposed data, including a bash history file with comments in Farsi, outlined the operator's process, which involved setting up a network, developing DDoS tools, and building out the botnet. The core of the infection strategy was a Python script that attempted to open 500 concurrent SSH sessions using a list of stolen credentials. Once successful, it would download the C-language source code for the bot client, compile it directly on the victim's machine to evade detection, and then launch the newly created bot, which would register itself with a hardcoded command-and-control server.

The infrastructure itself served a dual purpose, functioning as both an attack platform and a commercial VPN relay service designed to bypass Iran's internet filtering. The network consisted of servers in both Iran and Finland, linked by a shared security certificate. The bot client was designed for persistence, with built-in logic to continuously try and reconnect to its C2 server, ensuring infected machines remained under the attacker's control. The operator also had a "kill switch" script, allowing them to remotely terminate all botnet activity across every infected machine at once.

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/