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 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

MILITARYWATCH: CHINESE NAVY'S RARE J-11BSH LONG RANGE FIGHTERS TRAIN FOR MARITIME OPERATIONS

The Chinese People's Liberation Army (PLA) Navy's Southern Theatre Command has been conducting training exercises with its J-11BSH fighters, a rare twin-seat, long-range aircraft. This command is tasked with operations in the critical regions of the Taiwan Strait and the South China Sea. Due to the strategic importance of this area, which includes protecting major economic centers like Guangzhou and Shenzhen as well as the nuclear submarine base on Hainan Island, the Southern Theatre Command is often given priority for receiving the latest military equipment.

The J-11B, which entered service in 2009, is a significantly upgraded Chinese derivative of the Soviet Su-27 Flanker. It features superior engines, a lighter airframe due to increased use of composite materials, and more advanced avionics. The twin-seat J-11BSH naval variant serves as both a training platform and a command and control aircraft, taking advantage of the original Su-27 design's exceptional range for extended maritime missions. Enhanced versions, known as the J-11BGH, were introduced in 2021 with "4+ generation" technology, including an active electronically scanned array (AESA) radar. This modernization allows the aircraft to carry highly advanced PL-15 and PL-10 air-to-air missiles, which were initially developed for the J-20 fifth-generation fighter.

Although now overshadowed by newer designs, the J-11B played a crucial role as a stepping stone that helped advance China's fighter industry and bridge technological gaps with the West. The aircraft continues to be a significant part of the PLA's arsenal, with modernizations indicating it will remain in service for many years. Its successor, the J-16, has been produced in even larger numbers for the Air Force. The continued operation of the J-11B occurs as China rapidly expands its fifth-generation fleet and develops sixth-generation fighters, highlighting the dramatic transformation and increased capabilities of its armed forces since the J-11B was first introduced.

THEDEFENSEPOST: TAIWAN ARMY TO TEST NEW WEAPONS IN LIVE-FIRE DRILL

The Taiwanese Army has announced it will conduct a live-fire exercise to assess combat readiness and integrate new weapon systems into its units. Army Commander Lu Kun-hsiu stated that the drill is designed to ensure commanders at all levels are clear on training priorities. In preparation for the exercise, units are undertaking tasks such as inspecting ammunition, performing equipment maintenance, and conducting community outreach.

This year, 2026, is expected to be a peak year for the delivery of key military hardware to Taiwan. The army anticipates receiving all 108 M1A2T tanks and 14 Volcano mine-laying systems. Additionally, 18 more High Mobility Artillery Rocket Systems (HIMARS) are scheduled to arrive, complementing the 11 systems already delivered and deployed. This follows the completed deliveries of TOW-2B and Javelin anti-armor missiles by the end of last year.

Beyond these ground systems, Taiwan is enhancing its broader defense capabilities through strategic acquisitions and technological partnerships. The National Chung-Shan Institute of Science and Technology (NCSIST) has partnered with Shield AI to develop AI-piloted unmanned systems, aiming to control multiple drones with a single operator. Taipei is also expanding its Patriot missile arsenal, and in a recent development, the U.S. awarded a contract to equip Taiwan's air force with advanced IRST21 Legion ES infrared search-and-track systems, which are designed to passively detect and track airborne threats at long ranges.

ARMYRECOGNITION: NORTH KOREA FORMALLY HANDS OVER 50 KN-25 600MM ROCKET SYSTEMS TO COMBAT UNITS

On the eve of the Ninth Congress of the Workers' Party of Korea, North Korea showcased the formal transfer of fifty KN-25 systems to its frontline military units. This event was framed as a symbolic gift from defense industry workers, blending military procurement with political theater to highlight the system's importance in North Korea's force modernization. The KN-25 occupies a strategic gray area, possessing characteristics of both traditional rocket artillery and more advanced short-range ballistic missiles, offering greater range and precision than older systems.

The KN-25, which North Korea calls a "super-large multiple launch rocket system," is classified by U.S. Forces Korea as a short-range ballistic missile due to its size, range, and quasi-ballistic flight path. First tested in 2019, it has demonstrated a range of up to 380 kilometers. The missile itself is a single-stage, solid-propellant weapon measuring 600mm in diameter and approximately 8.6 meters long, making it dimensionally closer to a ballistic missile than a conventional rocket. It is equipped with fins for in-flight maneuverability and a guidance system that suggests a high degree of precision, capable of resisting electronic interference. Deployed on mobile launchers, the KN-25 can fire in rapid succession and quickly relocate, making it a difficult target to counter.

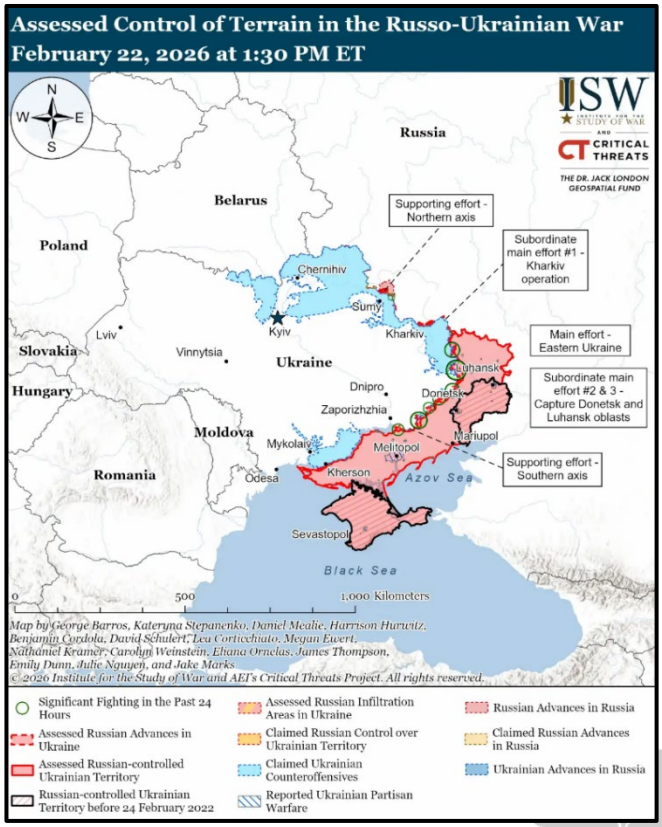
The fielding of fifty additional launchers signifies that the KN-25 has transitioned from a developmental system to a fully operational part of the Korean People's Army, indicating a scaled industrial production capacity. Strategically, it provides North Korea with a layered strike capability, able to target critical air bases, logistics hubs, and command centers throughout most of South Korea. Its ability to be fired in salvos can overwhelm missile defense systems like Patriot and THAAD. This development complicates regional security calculations for South Korea, Japan, and the United States, as it blurs the lines between conventional artillery and ballistic missiles, forcing a re-evaluation of defense architectures and counter-strike planning in a progressively intertwined political and military threat environment.

EUCOM

ISW: RUSSIA-UKRAINE UPDATE

Key Takeaways:

- Russian forces conducted another large, combined strike package overnight on February 21 to 22 and appear to be shifting their target set from primarily energy infrastructure to include Ukrainian water and railway infrastructure.
- Ukrainian officials accused Russian intelligence services of coordinating an improvised explosive device (IED) attack on a shopping center in Lviv City on February 22 that killed one and injured at least 25.
- Russia is likely escalating a sabotage campaign intended to degrade Ukrainians' trust in their security and destabilize Ukrainian society.
- Russia is reportedly selling man-portable air defense systems (MANPADS) to Iran, likely to repair its reputation among Iran and Russia's other allies.
- Russian forces recently advanced near Slovyansk.



THEDEFENSEPOST: IRAN, RUSSIA TO CONDUCT JOINT DRILLS IN THE SEA OF OMAN

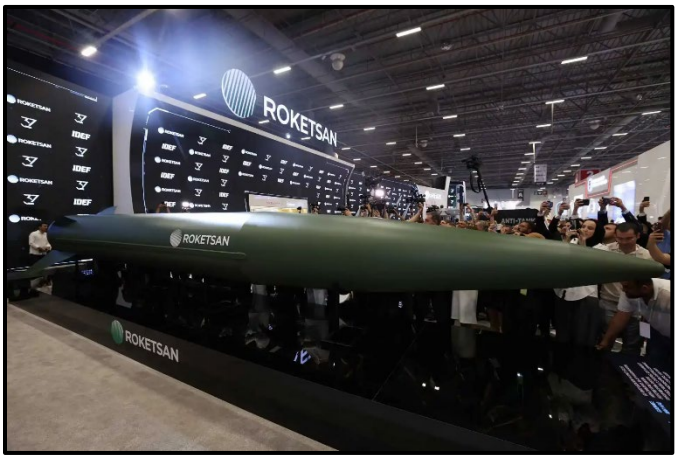
Iran and Russia are set to begin joint naval exercises in the Sea of Oman and the northern Indian Ocean. This development was announced shortly after a round of negotiations between Iran and the United States in Geneva. The new maneuvers follow separate exercises launched by Iran's Revolutionary Guards in the strategic Strait of Hormuz, which are seen as a direct challenge to the significant U.S. naval presence in the region.

According to drill spokesman Rear Admiral Hassan Maghsoudloo, the stated purpose of the joint Iran-Russia war games is to bolster maritime security and enhance the relationship between the two nations' navies. These military drills occur as Iran expresses optimism following the second round of talks with the U.S. which were mediated by Oman. Previous negotiations had fallen apart after an Israeli strike on Iran in June 2025 led to a brief war involving the United States.

The Strait of Hormuz remains a point of high tension and a critical channel for global oil and natural gas shipments. Amid the ongoing U.S.-Iran discussions, the area has regained prominence. Iranian officials have previously threatened to close the strait during heightened friction with the U.S. In a recent move, Iran announced it would partially shut the strait for several hours, citing security reasons related to its own military exercises.

ARMYRECOGNITION: TÜRKIYE'S TAYFUN BLOCK 4 HYPERSONIC MISSILE ENTERS SERIAL PRODUCTION IN 2026

Türkiye has officially announced that its next-generation TAYFUN Block 4 hypersonic ballistic missile will enter serial production in 2026. The confirmation came from defense analyst Turan Oguz and was later reinforced by ROKETSAN's General Manager, Murat İkinci. This development marks a significant achievement for Türkiye's domestic missile program, transitioning the weapon from the testing phase to industrial-scale manufacturing. The move signals that the missile has met the operational standards of the Turkish Armed Forces and will substantially enhance Ankara's long-range precision strike capabilities.



The TAYFUN Block 4 is a notable advancement over its predecessors, with classified upgrades to its propulsion, guidance, and terminal flight performance. While the original TAYFUN missile tested in 2022 had a range over 560 kilometers, the Block 4 is expected to approach or exceed a 1,000-kilometer range. Technologically, its designation as a hypersonic ballistic missile suggests advanced features, possibly including a refined propulsion system for a depressed trajectory and a maneuverable reentry vehicle. These characteristics would make it extremely difficult to intercept by modern air defense systems like the Patriot or S-400.

Strategically, the serial production of the TAYFUN Block 4 places Türkiye among a select group of nations with operational or near-operational hypersonic weapons, including the United States, Russia, and China. This capability serves multiple purposes for Ankara: it strengthens deterrence by providing a rapid and hard-to-intercept strike option, enhances strategic autonomy by reducing reliance on foreign weapon systems, and signals Türkiye's growing military-industrial maturity. The missile is expected to be deployed on mobile launchers to ensure survivability, reinforcing its role as a key pillar in Türkiye's national defense and altering the strategic balance in the surrounding regions.

CENTCOM

ISW: CENTCOM UPDATE

Key Takeaways:

- **U.S.-Iran Nuclear Negotiations:** Iran is unlikely to make any meaningful nuclear concessions in its upcoming draft proposal to the United States. Iran may calculate that it can delay the strikes if it offers a sufficiently conciliatory proposal, however.

- **Protests in Iran:** Iranians held 20 protests on February 20—one more than on February 19—which indicates continued public anger and frustration with the regime for its refusal to address the people's grievances. CTP-ISW recorded 20 anti-regime protests on February 20 across eight provinces at memorials that marked the end of the 40-day mourning period for protesters killed by security forces during the January 2025 protests.

- **Hezbollah's Participation in a Future Iranian Conflict with the United States or Israel:** Hezbollah may decide to participate in a future conflict between Iran and the United States or Israel if Hezbollah perceives that the U.S. or Israeli war aims seek to topple the Iranian regime. CTP-ISW has identified multiple courses of action Hezbollah may take in the event of a U.S. or Israeli strike on Iran.

MILITARYWATCH: IRAN DEPLOYS RUSSIAN S-300 LONG RANGE AIR DEFENCES AROUND CAPITAL

Iran has redeployed its S-300PM-2 long-range air defense systems to protect its capital, Tehran, and the city of Isfahan, amid a significant U.S. military buildup in the region. The S-300PMU-2 is a highly capable system, a direct predecessor to Russia's S-400, which Iran acquired in 2016 after a previous deal for a less advanced model was canceled. The system is noted for its advanced 48N6DM missiles, which can travel at over Mach 14 to engage targets at ranges of up to 250 kilometers, providing a formidable area defense capability.

This deployment counters widespread Western reports from October 2024 which claimed that Israel had destroyed all of Iran's S-300 systems. While analysts disputed these claims at the time, an Iranian military official later confirmed in July 2025 that some air defense assets had been damaged during clashes in June 2025. According to Rear Admiral Mahmoud Mousavi, these damaged systems were promptly replaced using domestic resources and pre-stored units to maintain the security of Iran's airspace. This statement came alongside regional reports suggesting Iran might also be receiving new long-range air defense systems from China.

Despite their capabilities, the Iranian S-300 systems face significant challenges. Iran is known to have procured only two regiments' worth of the systems and has not received the Su-35 fighter jets that were expected to enhance their effectiveness. A major vulnerability is that several NATO members, including Greece and Turkey, operate related S-300 and S-400 systems, allowing Western and Israeli forces to train against them. The U.S. Marine Corps even conducted exercises in November 2025 specifically targeting the S-300PMU-2. While Iran develops its own Bavar 373 system, its decision to purchase the S-300PMU-2 in 2016 suggests the domestic option was not considered sufficient at that time.

DEFENSENEWS: SAUDI ARABIA BUYS C-27 CARGO PLANES FITTED FOR ARMED MARITIME PATROLS

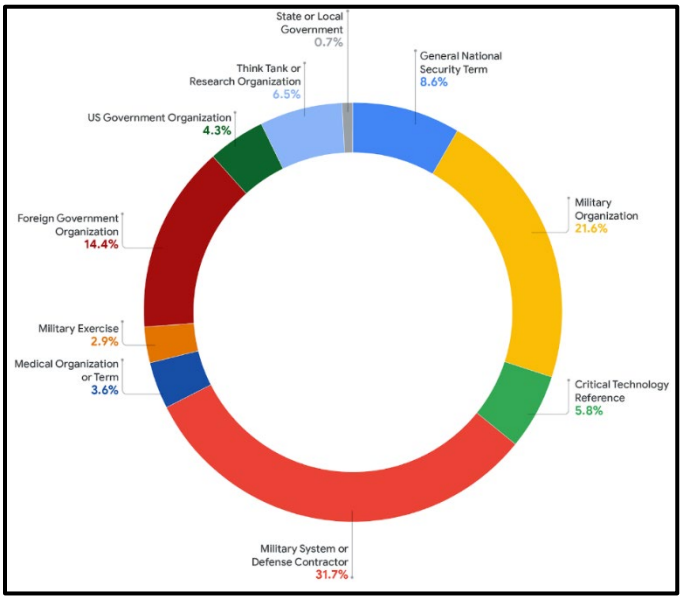
Saudi Arabia is set to become the first nation to use the C-27 tactical airlifter as an armed maritime patrol aircraft, according to an announcement from the manufacturer, Leonardo. The country will be acquiring four C-27Js specifically configured for this role. These aircraft will be capable of carrying torpedoes, anti-ship missiles, and depth charges, and will be equipped with a dedicated mission suite and advanced sensors to track targets both on the sea surface and underwater.

The aircraft are designed to be versatile, also performing search-and-rescue and air-drop missions. The Italian company, Leonardo, emphasized the platform's flexible design, which allows for the removal of the maritime mission consoles to convert the aircraft into a standard transport configuration. Deliveries of these specialized aircraft to the Saudi Navy are expected to commence in 2029. This purchase follows a previous acquisition by Saudi Arabia of two C-27Js for firefighting, cargo transport, and medical evacuation missions.

The C-27J, a smaller version of the C-130 designed to operate from short runways, has been sold to 19 countries. While the U.S. Coast Guard uses it for maritime patrol, it has not been sold as an armed variant until now. Potential weapons for the Saudi aircraft include the MBDA Marte-ER anti-ship missile and the MU-90 lightweight torpedo. Coinciding with this, a Leonardo-owned company recently signed a 200 million euro deal to supply Saudi Arabia with the MU-90 torpedo. Additionally, Leonardo is developing a special forces version of the aircraft, the MC-27, which will feature a side-mounted gun and is expected to be ready for sale between 2029 and 2030.

CYBERCOM

THEHACKERNEWS: GOOGLE TIES SUSPECTED RUSSIAN ACTOR TO CANFAIL MALWARE ATTACKS ON UKRAINIAN ORGS



A newly identified threat actor, suspected by the Google Threat Intelligence Group (GTIG) to have ties to Russian intelligence, has been systematically targeting Ukrainian organizations with malware known as CANFAIL. Initially focusing on defense, military, government, and energy sectors, the group's scope has since broadened. Their interests now include aerospace, manufacturing firms with military and drone connections, nuclear and chemical research facilities, and international bodies involved in conflict monitoring and humanitarian aid within Ukraine.

This actor, while considered less sophisticated and resourced than other Russian state-sponsored groups, has recently started leveraging large language models (LLMs) to enhance their capabilities. They use LLMs for reconnaissance, to craft convincing social engineering lures, and to find answers for technical challenges related to post-compromise activities. Their campaigns often involve impersonating legitimate entities, such as Ukrainian and Romanian energy companies, in phishing attacks designed to steal email credentials, and they have also been observed conducting reconnaissance on organizations in Moldova.

The group's attack methodology involves using LLM-generated content in phishing emails that contain Google Drive links to a malware known as CANFAIL. This malware is a disguised JavaScript file that executes a PowerShell script to download a memory-resident dropper, while simultaneously displaying a fake error message to the victim. GTIG has also linked this actor to a previously disclosed campaign called PhantomCaptcha, which used similar phishing techniques to deliver a different WebSocket-based trojan to organizations involved in Ukraine's war relief efforts.

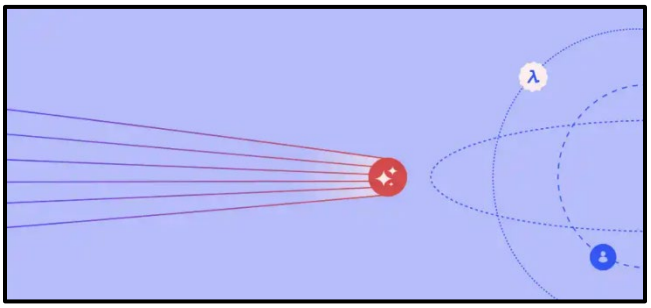
CYBERSECURITYNEWS: DELL 0-DAY VULNERABILITY EXPLOITED BY CHINESE HACKERS SINCE MID-2024 TO DEPLOY MALWARE

A newly discovered zero-day vulnerability in Dell RecoverPoint for Virtual Machines is being actively exploited in a critical campaign attributed to a suspected Chinese-nexus threat group known as UNC6201, which has overlaps with the group Silk Typhoon. The vulnerability, identified as CVE-2026-22769 and rated with a maximum severity score of 10.0, has been exploited since at least mid-2024. Attackers are leveraging this flaw to move laterally within compromised networks, establish persistent access, and deploy a trio of sophisticated malware: SLAYSTYLE, BRICKSTORM, and a new backdoor named GRIMBOLT.

The root of the vulnerability lies in a major security oversight within the appliance's Apache Tomcat Manager configuration. Researchers found hardcoded default credentials for the administrator account stored in a publicly accessible file. This allows unauthenticated remote attackers to log into the Tomcat Manager and abuse its software deployment function. In the observed attacks, this access was used to upload a malicious WAR file, which in turn deployed the SLAYSTYLE web shell, ultimately granting the attackers root-level command execution on the compromised Dell appliance.

UNC6201 has demonstrated advanced tradecraft, evolving its toolset by replacing the BRICKSTORM backdoor with the more evasive GRIMBOLT malware. GRIMBOLT is compiled using Native Ahead-of-Time (AOT) compilation, which strips out metadata that security tools typically inspect, making it harder to detect. The attackers also employ sophisticated networking tactics to remain hidden, creating temporary, hidden network ports called "Ghost NICs" to pivot silently across networks. Furthermore, they use a technique known as Single Packet Authorization (SPA) to conceal their command and control channel, only allowing connections on a specific port after receiving a secret "magic packet," effectively hiding their traffic from standard network monitoring.

THEHACKERNEWS: FROM EXPOSURE TO EXPLOITATION: HOW AI COLLAPSES YOUR RESPONSE WINDOW



In 2026, the landscape of cybersecurity has been fundamentally altered by the speed and scale of artificial intelligence. Minor operational security risks, such as a developer granting overly broad permissions or an engineer forgetting to revoke a temporary API key, are no longer manageable debts to be addressed later. AI-powered adversarial systems can now discover, map, and simulate thousands of attack paths against these vulnerabilities in a matter of minutes. This compression of reconnaissance and exploitation has shattered the traditional timeline that once favored defenders, with a significant percentage of vulnerabilities now being exploited on or before the day they are publicly disclosed.

Attackers are leveraging AI in two primary ways: as an accelerator for traditional attacks and by targeting AI infrastructure itself as a new attack surface. As an accelerator, AI automates the chaining of low and medium-risk vulnerabilities into viable attack paths, exploits the massive sprawl of machine identities to move laterally within networks, and enables highly convincing, context-aware phishing campaigns at an unprecedented scale. Concurrently, attackers are targeting organizations' own AI systems through prompt injection, tricking internal agents into exfiltrating sensitive data, and poisoning AI memory with false information to create dormant insider threats. They even poison the software supply chain by predicting and registering malicious packages that AI coding assistants are likely to suggest to developers.

To counter this AI-driven threat, organizations must shift from traditional, reactive security measures, which are too slow and overwhelmed by noise, to a proactive strategy of Continuous Threat Exposure Management (CTEM). This approach focuses on identifying and remediating the specific exposures that can be chained together to form a viable attack path to critical assets. Instead of counting alerts and patches, the goal is to find the convergence points where a single fix can sever dozens of potential routes for an attacker. By focusing on closing these critical pathways faster than an AI can compute them, defenders can reclaim the window of exploitation and effectively manage risk in the new era of AI-accelerated threats.

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/