

Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Federal Department of Defence, Civil Protection and Sport DDPS **armasuisse** Science and Technology

DEFTECH-SCAN

January 2025





deftech.ch/scans





Dear Reader,

We are always on time to wish you a wonderful 2025 !

You will discover in the release, in the background and because of the recent release of <u>DeepSeek</u>, which would definitely be of support for the chapter 1.2, a huge presence of China. This was not a planned focus per se, but some of the announcements made in the last two months confirmed that looking at timeless themes such as <u>invisibility</u>, trust, etc. help connecting the dots when it comes to putting "weak signals" into contexts.

We would also take the opportunity to introduce and promote the study "<u>China's remote sensing</u>" coordinated by Tate, which implications are also part of chapter 6 :

As we prepare for what's next, take a look at these major news:

1.	Applications of AI and data2
2.	Robotics and Autonomous Systems4
3.	Connectivity7
4.	Human Protection and Performance12
5.	Platforms and Weapons Systems14
6.	Space

CHINA'S REMOTE SENSING	
Submitted to the U.S. China-Economic and Security Review Commission	
OTH Intelligence Group LLC Tate Nukic, Christma La Maro, Coris Rando, Bophen Rodriguer, Hassan Atanak, Andrew Gonzale Reviewed by Bocca Wasser	December 2024
Notation: This means of more an gamping by Chi Budigano Gampi Li a distances from a first children and the children and the second second advances from a distance of the second second second second second environment of the second	

We wish you an interesting read.

Foresightly Yours,

Tate I

OTH Intelligence Group CEO tate.nurkin@othintel.com

Dr. Quentin Ladetto

armasuisse S+T Head of Technology Foresight quentin.ladetto@ar.admin.ch





1. Applications of AI and data

1.1	India establishes AI incubation centre
	The Indian Army is collaborating with Bharat Electronics Limited (BEL) to launch the Indian Army AI Incubation Centre (IAAIIC) in Bengaluru (<u>source, source</u> and <u>source</u>)
	Assessment: On 21 December, Indian Army Chief General Upendra Dwivedi formally opened the IAAIIC via a virtual ceremony. The centre is part of India's on- going efforts to build a technological advanced force with a robust AI infrastructure that relies on domestically developed technologies and capabilities.
	Specifically, the centre will focus on driving research and development on several identified priority areas, including predictive maintenance, enhanced surveillance, decision-support systems, and autonomous platforms. India joins a growing list of nations that have recently announced the establishment of military AI research and development centres that create forums for collaboration between the government, traditional defence industry players, and start-up technology companies, including Japan and South Korea, which both established such centres in 2024.
	Also during the reporting period, <i>India Today</i> reported that Indian Army officials were already using AI-enabled capabilities to enhance its intelligence, surveillance, and reconnaissance (ISR), logistics, and cybersecurity operations. Unnamed Army officials told the outlet that "AI-powered drones and satellite systems are being used for intelligence gathering, providing real-time data for strategic decision-making. In logistics and supply chain management, AI algorithms can optimize supply chain operations, ensuring timely delivery of essential resources to the frontline." The officials also highlighted the utility of AI for cybersecurity and in developing more realistic synthetic training environments.





1.2	War winner? US to test generative AI in operational decision-making in Indo- Pacific
	The US Department of Defense (DoD) is partnering with Palantir and Anduril to explore how generative AI can help commanders make battlefield decisions more quickly against advanced adversaries or in complex contingencies. (<u>source</u> , <u>source</u> , and <u>source</u>)
	<u>Assessment</u> : The initiative will focus on helping the US Indo-Pacific Command explore the utility of generative AI in naval use cases to "drive down the time down and increase the decision space for commanders" in the region, according to Radha Plumb, the head of the DoD's Chief Digital and Artificial Intelligence Office (CDAO). DoD is partnered with Anduril and Palantir, two large defence technology firms that have expanded their business with and influence in DoD over the last several years. One industry official described the initiative as not being a single new product or tool, but "a framework between a consortium of next generation technology companies and commanders to better understand how they might use generative AI in operations—and then either building what they need or refining tools that already exist."
	The testing and experimentation will last for 90 days. CDAO has previously explored how generative AI can be used to support military healthcare, logistics, administrative tasks such as writing contracts. This effort marks the first time CDAO has tested the applicability of cutting-edge generative AI tools to accelerate the time it takes for commanders to gain a shared situational awareness and issue commands during a conflict.
	One potential challenge with this generative AI application is the amount of computing power needed to incorporate AI into operations. Plumb told <i>Defense One</i> that "the better models require a lot of compute resources in order to do the kinds of inference things we want them to do. That's because they're pulling across a wide range of data sources. So, they need to pull all those data sources in, especially if we want to tweak them via things like fine tuning or augmentation onto DoD-specific contexts."
	The announcement comes on the heels of the revelation in December that Anduril and Palantir will seek to work more closely together to support DoD on a number of projects. The two companies also pledged to lead a broader consortium of technology and software companies to jointly pursue DoD business in an attempt to gain a competitive edge over US defence primes and traditional contractors. In the weeks leading up to the announcement, Anduril formed partnerships with Oracle and autonomous system maker Arrow while Palantir has expanded its partnership with Shield AI and established a partnership with Booz Allen Hamilton to develop AI tools for logistics, autonomous systems, and other capabilities.





2. Robotics and Autonomous Systems

.2.1	Sweden unveils drone swarm capability to support ground troops
	An announcement from Swedish Minister for Defence reflects growing interest in leveraging the advantages of masses of small uncrewed aerial systems (UAS) in supporting ground forces in a range of key tasks (<u>source</u> and <u>source</u>)
	<u>Assessment:</u> The 15 January announcement was accompanied by the provision of a demonstration video to <i>Defense News</i> that provides more detail on how the Swedish swarms are designed to work. The video shows a formation 10 quadcopters taking off and relaying footage of their flight trajectory to ground operators. A voice over explains that the drones' high-resolution imagery and artificial intelligence-driven analyses allow commanders to make better and faster decisions based on more timely and accurate situational awareness.
	Swedish company Saab is developing software for the drones and working closely with the Swedish military, the Swedish Defence Material Administration, and the Swedish Defence Research Agency. According to a Saab representative, "the individual [UAS] in the swarm are equipped with different capabilities, such as varying sensors, payload, and communication capacities—the swarms are controlled by a single operator who can assign tasks to one or more swarms for instance via a mobile phone."
	The concept of one operator controlling a swarm of several drones with complementary and redundant capabilities is becoming more of a reality on the modern battlefield, especially as control technologies and interfaces become more sophisticated. An Atlantic Council report entitled Missiles, AI, and drone swarms: Ukraine's 2025 Defense Tech Priorities states that "Ukraine's drone units are already beginning to move beyond the initial concept of 'one drone, one operator,' and will be looking to transition toward more widespread use of drone swarm technologies in 2025." Saab has suggested that other Nato allies have expressed interest in the capabilities. Sweden will conduct additional tests on its emerging drone swarm capabilities during the Arctic Strike exercise in March 2025.





2.2 Uncrewed systems taking a larger role in maritime countermine mission The reporting period saw two notable reveals of uncrewed systems designed to carry out maritime mine detection and defeat. While some countries still prefer to use these robots to support human operators in counter-mine missions, more countries are looking to rely on uncrewed systems while keeping humans outside of the operating zone. (source, source, and source) Assessment: In late October 2024, Turkish shipbuilder STM launched an indigenously developed uncrewed underwater vehicle (UUV) known as the NETA 300, which is the first in an expected family of UUVs. The NETA 300 has been developed at least initially for the underwater countermine mission. A company statement said that "the system operates autonomously when deployed for Mine Countermeasure (MCM) Operations, making use of side-scan and gap-filling sonar technologies to identify mines in suspected high-risk areas. This enables the user to classify and identify mines or mine-like objects as quickly and effectively as possible." However, the company also advertises that the NETA 300 is built on modular design principles that will allow it to carry out a range of both military and commercial-focused missions including intelligence, surveillance, and reconnaissance (ISR), anti-submarine warfare, and pipeline and geographic surveys. The system has a maximum speed of 5 knots and maximum operating life of 24 hours on a single battery charge and can be deployed in shallow waters up to 300 meters deep. It is currently in pool and sea testing phases. The development reflects growing interest in the use of uncrewed systems for the dull, dirty, and exceptionally dangerous mission of maritime countermine operations. On 12 November, Thales announced it will provide the French Navy with its first production of an autonomous mine-hunting system by the end of 2024 as a first step to transitioning to fully remote countermine capability. The systems for France and the U.K. include a portable operations centre, uncrewed surface vehicles using detection methods including towed sonar, and a remotely operated vehicle to neutralize mines. Autonomous functionality in the system includes deployment and operation of payloads, as well as navigation by the unmanned surface vehicles. According to Defense News. France and the UK are among a group of companies moving to fully stand-off countermine operations, along with the Netherlands, Belgium, and the United States. This option has only become possible in the recent past as the technology around autonomous and uncrewed systems has advanced. However, not all countries are making this move. Other countries, including Italy and Germany, see value in maintaining a crewed mine-hunting capability. But even these approaches rely on uncrewed systems to help detect and disable maritime mines reducing risk to crewed vessels in maritime mine fields.



Figure 1: The STM NETA 300 on display at SAHA EXPO 2024 in Istanbul





2.3	Maritime Streetlights: NATO planning uncrewed fleet to monitor undersea cables
	The announcement follows a series of acts of sabotage against underwater critical infrastructure in the Baltic Sea and North Atlantic. (<u>source</u> and <u>source</u>)
	<u>Assessment</u> : Admiral Pierre Vandier, NATO's Supreme Allied Commander Transformation told <i>Defense News</i> that the Alliance was planning to launch a fleet of uncrewed surface vessels (USVs) to increase monitoring of and presence around critical undersea infrastructure such as gas lines and communication cables. Admiral Vandier likened the planned capability to CCTV cameras mounted on streetlights in areas of high crime to either capture threatening activity, telling the outlet that "the technology is there to make this streetlighting with USVs." The new fleet is not yet fully developed, though it is expected to be ready before the NATO summit in June. It is unclear what types of USVs will be developed and deployed
	Enhancing maritime security and protection of undersea critical infrastructure has become a priority for NATO member states, especially those in Northern Europe and Scandinavia. Attacks on undersea cables and gas pipelines have increased since Russia's invasion of Ukraine in February 2022, including a suspected act of sabotage against two undersea fibre-optic cables in November 2024.



Figure 2: A map showing the navigation pathways of two ships—the Norwegian flagged Silver Dania and Barbadian flagged Pskov suspected of sabotaging an underwater data cable in the Baltic Sea in one of a growing number of similar incidents in the region. The Silver Dania had recently left Russia while the Pskov was sanctioned by the United States on Jan. 10 because it is suspected of being part of the so-called shadow fleet that helps Russia transport oil and gas. Source: Source: MarineTraffic (vessels); TeleGeography (cables), and Emma Brown, <u>Wall Street Journal</u>





3. Connectivity

3.1	The "Invisible Battlefield": The electronic warfare competition in Ukraine
	<i>Wired</i> profiled how Ukrainian and Russian forces are approaching the battle for the electromagnetic (EM) spectrum, emphasizing the importance of signals jamming, counter-drone weapons, and defensive electronic warfare to success on the battlefield. <u>(source</u>)
	<u>Assessment</u> : Published on 23 December, the in-depth article profiles the ways in which iterative innovations in electronic warfare (EW) are shaping the conflict in Ukraine, ultimately concluding that the two sides are "fighting to electromagnetic stalemate."
	One central component of the EW conflict is the competition to, on one hand, intercept, jam, and spoof communication, radar, and data transmission signals and, on the other hand, protect these signals from compromise. Effective implementation of EW has the potential to negate technological or capability advantages by greatly reducing the effectiveness of military equipment that relies on the EM spectrum to detect, navigate, communicate, or transmit.
	Ukraine's strategy in this competition has revolved around producing a large number of more affordable EW systems and making them adaptable and easily upgradable as Russia creates its own new EW capabilities to counteract those of Ukraine. Examples include the Bukovel AD counter-drone system that can be mounted on the back of a pick-up truck and the Eter system, which is the size of a suitcase and can detect Russian jamming signals, allowing Ukraine to target Russian EW units with artillery.
	Ukraine has also instituted decentralized, distributed EW solutions. For example, Ukraine has developed a "secretive mesh network of EW systems" to counter Russia's Iranian-made Shahed drones, which have demonstrated the ability to manoeuvre through Ukrainian air defences. Oleksandr Fedienko, a Ukrainian politician told <i>Wired</i> "it's not one, not two, not three transmitters. There are hundreds of thousands of devices that are installed throughout the country" to detect, jam, and even spoof incoming threats. In recent months, Ukrainian forces have reportedly been able to spoof the signals of dozens of drones, flying more than 100 back into Russia as well as navigating Russian drones safely to the ground behind Ukrainian lines so that they can be analysed to better calibrate EW and air defence responses in the iterative and evolving electronic attack and defence contest.



Т



3.2	China claims "world's first" in military 5G connectivity
	China's People's Liberation Army (PLA) and China Mobile Communications Group co- developed what is being described as the world's first mobile 5G base station, which is now reportedly ready for deployment. (<u>source</u>)
	<u>Assessment:</u> A peer-reviewed paper published on 17 December in the Chinese journal <i>Telecommunications Science</i> by a senior engineer with the 31567 Unit of the PLA revealed that the organization has developed a mobile 5G station. According to <i>South China Morning Post</i> , the system provides "unprecedented high-speed, low-latency and extremely secure and reliable data exchange to at least 10,000 users within a 3km radius." The article points out that in the PLA context, the 10,000 users are likely to be drones. Even while on the move or operating in complex, contested, and congested terrains, the system reportedly can maintain uninterrupted throughput of 10 gigabits per second and a latency of less than 15 milliseconds.
	The system involves a platform that can be mounted on the top of a military vehicle that houses three to four drones. The drones serve as the 5G base station and can take off alternately as deployed forces manoeuvre, providing continuous connectivity. As an individual drone's battery becomes low, one of the other drones can be launched to replace it while the original drone returns to the vehicle for charging.
	The development of mobile 5G with reduced vulnerability to electronic warfare could be an enabler of the large-scale use of autonomous systems. To date, use of large numbers of interconnected drones has been limited in some contexts by communication technologies that cannot meet the massive data exchange demands required for the use of thousands of autonomous systems.
	The article states that the PLA has conducted "many tests" on the system and is now being considered for "safe, reliable, rapid deployment." Lockheed Martin and large US-based telecommunications company Verizon have also collaborated to build a similar system, though it is at an earlier stage of development and, according to the PLA authored paper, does not have the same low levels of latency as the PLA system.





3.3	Lithuania establishes new Cyber Defence Command
	The move consolidates most cybersecurity responsibilities under Lithuanian Cyber Command (LTCYBERCOM) to enhance the country's cyber and critical infrastructure security and ensure interoperability with allies. (<u>source</u> and <u>source</u>)
	<u>Assessment:</u> On 1 January the Lithuanian Ministry of National Defence officially inaugurated the LTCYBERCOM in an effort to address the growing range of cyber threats to Lithuania's military, civil government activities, population, and infrastructure. The creation of LTCYBERCOM is designed to consolidate more of the country's cyber defence resources under a single authority and to increase interoperability with NATO allies, many of which have already established similar cyber-focused commands.
	The command will include:
	 A headquarters responsible for planning and implementing cyber operations
	 The Lithuanian Great Hetman Kristupas Radvila Perkunas CIS Battalion, which will provide communication and information services throughout the defence structures; and
	The Cyber Defence Command's IT Service
	While this move is part of an effort to consolidate cyber activities, some tasks will be transferred to the National Cyber Security Center and Core Centre of State Telecommunications, both of which also fall under the Ministry of National Defence. The National Cyber Security Center will serve as the national cybersecurity agency, providing cyber incident response and resilience across government entities and key sectors. Its activities will complement those of the LTCYBERCOM.
	Cybersecurity threats have increased in recent years, in part due to the diplomatic and materiel support most NATO members have provided Ukraine after Russa's invasion of the country in February 2022. In 2023, <u>Google reported</u> a significant increase in Russian cyberattacks targeting NATO countries since the invasion began. NATO <u>has established a new defence facility</u> in Europe in response as part of effort to provide coordinated alliance-wide protection to member states.





3.4 By the stars: Australian researchers develop a vision-based navigation system The system uses visual data from stars to navigate in a GPS-denied environment,

offering a simpler more cost-effective star-based navigation system than those that have been used previously. (source and original research paper)

<u>Assessment:</u> Researchers at the University of South Australia have developed a system that employs an algorithm that analyses star-based visual data via standard autopilot system for nighttime navigation in GPS-denied environment.

Testing on a fixed-wing drone achieved accurate positioning within 2.4 miles / 4kms. The system could fill a gap in star-based navigation systems for small drones, which cannot use the large and complex systems in use for bigger aircraft. According to a researcher on the University of South Australia team, "unlike traditional star-based navigation systems, which are often complex, heavy, and costly, our system is simpler, lighter, and does not need stabilization hardware, making it suitable for smaller drones." The lightweight strap-down celestial navigation systems use cameras to track stars and algorithms to estimate the position based on star elevation and attitude data.

The main limitation of the system is accuracy as even small attitude errors in lowcost autopilots can lead to large positional inaccuracies, though this is expected to improve as computer vision technologies advance. The system's performance will also be affected by weather and visibility conditions. The research team released a statement that the capability is "ideal for operations over oceans, or in warfare zones, where GPS jamming is a risk. Apart from the defence sector, it could also be highly useful for environmental monitoring."





Figure 3. Platform layout of the autopilot and celestial payload within the airframe.

Figure 3: An image of the celestial payload (left), consisting of a Raspberry Pi 5 and an Alvium 1800 U-240 monochrome sensor fitted with a 6 mm f/1.4 wide angle lens, and the layout of the autopilot and celestial payload on the drone used during the 72-minute test flight. Source: <u>Original research paper</u>





3.5	It's about time: UK develops quantum clock to improve resilience of ISR assets
	The Defence Science and Technology Lab (DSTL) revealed it has built a quantum clock to improve precision, navigation, and timing (PNT), making it the first quantum clock built in the UK (<u>source</u>)
	<u>Assessment:</u> On 2 January, DSTL announced that it has built a quantum clock that will reduce the reliance of ISR assets on global navigation satellite systems (GNSS) like GPS, which are increasingly attractive targets for jamming and spoofing.
	According to the UK MoD, the clock's precision is "so refined that it will lose less than one second over billions of years, allowing scientists to measure time at an unprecedented scale."
	Quantum clocks offer several advantages for the military, including:
	 Enabling more precise and independent navigation systems
	 Reducing the reliance of navigation systems on GNSS
	 Increase the security of communications systems, including encrypted military networks, which rely on highly synchronized timekeeping
	 Improve the accuracy of weapons systems, which rely on accurate timing to calculate trajectories and coordinate attacks
	 Improve the ability of forces to operate in "timing critical operations", such as cyber operations, "where milliseconds can make a difference."
	The development of DSTL's quantum clock is part of the UK Government's broader Plan for Change effort, which seeks to enhance the UK's national security while also supporting skilled and productive jobs.
	The quantum clock is expected to be deployable in military operations in the next five years and will undergo further research to decrease the system's size and enable mass manufacturing.





4. Human Protection and Performance

4.1	The end of the "Golden Hour"? Battlefield evacuation of wounded complicated by new technologies
	The emergence of drones and other battlefield technologies are reducing the ability of militaries to evacuate wounded soldiers in a timely manner, driving new requirements for military medicine. (source and source)
	<u>Assessment:</u> Reporting from <i>Business Insider</i> detailed how the increased use of UASs in combat is complicating the task of timely battlefield evacuations, especially those taking place within the first 60 minutes of a soldier being wounded—a period of time commonly referred to as "The Golden Hour." The prevalence of surveillance drones and the inability to establish air superiority in a highly contested environment means that ground evacuations are likely to be detected and targeted and those by helicopter will be vulnerable to enemy air defence fire.
	Challenges with timely evacuation of wounded has been an increasingly prominent feature of the Ukraine war. Soldiers are frequently forced to wait for a break in fighting to be evacuated, contributing to increases in combat deaths and serious wounds. One U.S. Army veteran fighting in Ukraine reported that "here in Ukraine, we have a golden three days." The low light of dusk and dawn also provide an opportunity to get wounded soldiers away from the front line as Russian forces switch out "their surveillance drones from normal analogue video to either thermal or night vision."
	While some view this disruption as a "paradigm shift", other observers note that it is really a return to "the patterns and expectations of World War II operations and Cold War planning, exacerbated by current technology and lethality."
	Reinforcing the latter point about new technologies and lethality worsening the problem, Brigadier General Anthony McQueen, commander of the U.S. Army's Medical Research and Development Command told <i>Task and Purpose</i> in June 2024 that the wounds that need to be treated in Ukraine are different from those in Afghanistan and Iraq due to the weapons being deployed to Ukraine. "New types of weapons are being usedAre they creating different types of injuries? We need to make sure that we're linking up with those from a treatment standpoint and from a wound care and bandage standpoint.





4.2	Chinese Researchers claim advancement in adaptive camouflage technology
	In a published study, researchers claim to have developed a material that changes colour at a molecular level based on surrounding light, allowing individuals and potentially items or vehicles to better blend into their environment. (<u>source</u> —behind firewall—and <u>source</u>)
	<u>Assessment</u> : A team from the University of Electronic Science and Technology of China published a paper in the peer-reviewed journal Science Advances that details their development of a new technology that when applied to clothing "could make an individual effectively 'invisible."
	The technology relies on a process the researchers referred to as self-adaptive photochromism (SAP) during which a molecular compound changes its structure when it is exposed to specific wavelengths of light. To the human eye, the material appears to blend seamlessly with its environment.
	The team believes its approach is simpler than other man-made efforts to develop adaptive camouflage that can use complex electronic devices. The technology is applied as a coating that can be sprayed or applied to various surfaces, enabling adaptive camouflage on solid materials. The study emphasises that the material is relevant not just for camouflage but also for encryption and stealth technology. The team acknowledges that further research is required to mimic all colours within the visible light spectrum, particularly purple and blue.





5. Platforms and Weapons Systems

5.1	Boxing Day surprise! China stuns with two new aircraft designs
	Images of two previously unseen tail less designs on-line led to extensive speculation about the role and nature of the aircraft and alarm at the pace of advancement of China's military aviation capability among military aviation analysts, particularly in the United States. (<u>source</u> and <u>source</u>)
	<u>Assessment</u> : On 26 December, images of what appear to be two sixth generation fighter aircraft prototypes sent China watching communities around the world into a frenzy. While much about the aircraft are still unknown, the appearance of the two designs constitutes a significant development in China's military aviation and indicates increasing capacity for and accelerating pace of technological innovation.
	The first plane to make an appearance on-line—and the one about which there is more information—is being referred to as the J-36. It features a diamond wing tailless configuration with prominent leading-edge extensions blending seamlessly into the nose section.
	The stealthy plane is notable first for its size, presenting as much larger than the Chinese J-20 chase plane also shown in some photographs of the J-36. The increased size reduces agility but also increases payload and provides an indication that its mission may be as a long-range multi-role aircraft capable of penetrating enemy air defences, performing air-to-air missions, and striking ground targets. Another interesting component of the design is the use of three engines, with two intakes mounted on the bottom of the aircraft and one prominently mounted dorsally. This design will increase thrust.
	Less is known about the second aircraft. While smaller than the J-36, this aircraft is still in the heavy fighter class. It appears to be a multi-role air dominance fighter aircraft, though with less range than the J-36. It is assessed to be larger overall than the J-20 and more efficient with a lower overall signature.
	The story was covered extensively in defence and aviation media, though perhaps the most exhaustive coverage was produced by <i>The War Zone</i> , which documented each aircraft's specifications and attributes and provided analysis of the aircrafts' potential roles and implications. Despite the extensive coverage, there remains uncertainty about the status of both plane's development. Most assessments find that this was likely the first flight for both, meaning that they are both likely technology demonstrators or early prototypes rather than aircraft that are approaching production.
	Some analysis of the implications of the existence of these aircraft have focused on the reveal in the context of China-United States military competition. Many analysts have pointed out that the reveal of these two purported 6 th generation aircraft come at precisely the time that the U.S. Air Force has paused to reconsider its approach to its 6 th generation Next Generation Air Dominance (NGAD) program in order to better understand program requirements. While the comparison is certainly valid, it is also worth noting that the U.S. Air Force did reportedly fly an NGAD prototype in 2020, though no images were released of the flight. Nonetheless, the flights of the Chinese aircraft do constitute a significant development reflecting the accelerating pace of China's military technological innovation and efforts to achieve technological dominance in military aviation.







Figure 4: Images of the two aircraft released on December 26, 2024. The top two images are of the J-36 while the bottom two are of the yet unnamed second aircraft. The bottom image shows the second aircraft being pursued by a Chinese J-20 fifth generation fighter





6. Space

6.1	Commercial remote sensing of growing interest to defence communities
	Multiple developments in the reporting period demonstrated and explored the growing connections between commercial remote sensing capabilities and defence and security capabilities and missions. (source and source)
	<u>Assessment:</u> On 9 January, U.S. commercial space-based remote sensing company Maxar announced it had signed a \$14.4 million deal with the Dutch military to provide access to Maxar's satellite tasking capabilities, imagery archive, and data analytics through its Geospatial Platform Pro service. The contract will support hundreds of users at the Dutch Defence Geographic Agency conducting mapping, intelligence, and operational support missions. Maxar's general manager for international government told <i>Space News</i> that "as many NATO countries look to build up their own sovereign geospatial intelligence capabilities, they're turning more and more to commercial partners."
	This trend is attributable first and foremost to the value that space-based remote sensing can provide to defence and security communities around the world, including providing accurate topographic and bathymetric mapping, enhancing surveillance and reconnaissance, monitoring change detection, crisis monitoring and supporting improved PNT, among other uses. However, developing a robust and resilience space-based remote sensing infrastructure can be expensive to develop and maintain. The proliferation of commercial space-based remote sensing companies throughout the world such as Maxar, BlackSky, ICEYE, and others provides a lower cost means of accessing relevant imagery and data to augment other more expensive or classified remote-sensing capabilities.
	A report published in December 2024 through the U.SChina Economic Security and Review Commission provided an in-depth analysis of China's remote sensing capability. The wide-ranging report (author's note: the author of this scan was involved in the production of the <i>China's Remote Sensing</i> report) looks at several aspects of China's growing remote sensing ecosystem and its motivations for developing a more robust remote sensing industry, both in terms of space-based remote sensing and other applications of remote sensing such as in the autonomous vehicle and UAS markets.
	The report includes a case study tracking the growth of China's largest commercial remote sensing company, CGSTL, which is currently developing the largest known commercial space-based remote sensing constellation of 300 satellites in Low Earth Orbit (LEO). The company is one of two Chinese remote sensing satellite companies to have been sanctioned by the US government for selling images and satellite access to the Wagner Group in support of the group's operations in Ukraine and Africa. CGSTL also reportedly has close ties to the People's Liberation Army, further demonstrating the increasing importance of commercial space-based remote sensing as a force multiplier for modern defence and security communities.

