

Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra

Federal Department of Defence, **Civil Protection and Sport DDPS** armasuisse Science and Technology

deftech.scan

December 2023



https://deftech.ch/scans







Dear Reader,

2023 is almost to its end and it is our pleasure to present you our last <u>deftech.scan</u> of the year.

We believe that if we have to remember something from the past 12 months is that nothing has to be considered as a given.

Technology will continuously support innovation and strategy to create surprise and provide an advantage to its user, being in a high-tech or low-tech environment or coming from military or civilian developments.

This is why constant monitoring of technologies and expected use has never been more important:

1.	Applications of AI and data	2
2.	Autonomous systems and robots	4
3.	Sensors	7
4.	Connectivity	9
5.	New Weapons	11
6.	Space	13

We wish you an interesting read and a happy holidays.

Foresightly Yours,

la

OTH Intelligence Group CEO tate.nurkin@othintel.com

Dr. Quentin Ladetto armasuisse S+T Head of Technology Foresight quentin.ladetto@armasuisse.ch





1. Applications of Al and data

1.1	AUKUS countries to use AI to track Chinese submarines
	Trilateral announcement made in California focuses on the use of AI to find and track China's expanding submarine force (joint statement and additional source)
	<u>Assessment</u> : The defence ministers of Australia, the United Kingdom (UK), and the United States (US) met in California on 1 December to discuss the AUKUS enhanced security and defence partnership.
	The AUKUS deal has received the most attention due to the agreement for the US and UK to help Australia build nuclear-powered attack subs. However, the deal also includes a second pillar—Pillar II—that focuses on collaboration on the development and use of emerging technologies, including AI.
	According to a joint statement, the three countries agreed to several actions and initiatives that reflect interest in the use of AI-enabled capabilities to meet the growing security and defence challenges of the Indo-Pacific.
	Most notably, the countries agreed to use AI technology on anti-submarine warfare systems, including the P-8 Poseidon aircraft, to process information relayed from sonobuoys (which detect and transmit underwater data), to improve the combined "anti-submarine warfare capabilities" of the three nations. The statement also included a commitment to continue to develop and deliver resilient and autonomous AI technologies to "enhance force protection, precision targeting, and intelligence, surveillance, and reconnaissance."
	The joint statement also included references to enhancing partner capability for undersea vehicle launch and recovery, quantum positioning, navigation, and timing, deep space advanced radar capability, and to increase AUKUS maritime autonomy experimentation and exercises designed to increase "the sophistication and scale of autonomous systems in the maritime domain."
	The three countries have expressed increasing concern over China's attempts to enforce maritime claims in the South and East China sea, especially activities taking place in international waters or in the territorial waters of other nations. Indeed, <u>Australian navy divers were injured in a November incident</u> in which one of China's naval vessels used sonar pulses against the divers who were clearing fishing nets from the propellers of the Australian frigate HMS Toowoomba. The incident took place in Japan's exclusive economic zone (EEZ).
	The undersea domain is an extremely important component of the intensifying military and geopolitical competition unfolding in the Indo-Pacific. The United States and its allies and partners have long held a significant advantage in undersea capability that is currently being challenged by the growing presence of more and more sophisticated and capable Chinese submarines and sensors, <u>as a 20</u>





1.2 Thales wins French Ministry of Defence CAID challenge

French company's "Friendly Hackers" team won the inaugural exercise designed to identify vulnerabilities in AI training data and models that adversaries can exploit to affect performance of AI-enabled military systems (source)

Assessment: The CAID challenge was held during the fifth edition of European Cyber Week in France (21 – 23 November). According to a Thales press-release, competing teams were asked to complete two tasks. First, teams were given a set of images and asked to determine which were used to train an AI algorithm and which were not. Identifying images used for algorithm training can help adversaries gain valuable information about the training methods used and the quality of the training model that can then be used to inform operations that target any perceived training vulnerabilities. Second, teams were asked to find images of aircraft used by an AI algorithm that had been protected or erased using "unlearning" techniques. Unlearning techniques involve deleting data used to train a model to reduce data security vulnerabilities. Most notably, unlearning can help ensure the integrity of an algorithm if it or the system it is enabling—a drone, for example—is lost, exported, or stolen. It can also ensure that classified or sensitive data used to train algorithms cannot be accessed by other actors, such as adversaries. Thales' team was able to reidentify data that was supposed to have been erased from the exercise's training model. Exercises like CAID are extremely valuable in ensuring resilience and reliability of AI-algorithms and the systems they enable, which are featuring more and more in military operations. By understanding the vulnerabilities associated with training data and models, militaries can take proactive steps to protect algorithm integrity and ensure adversaries cannot use backdoors to compromise underlying algorithms and alter or impair the performance of AI-enabled military systems.

1.3 Al-driven electronic defence capability debuts in European exercises

The US Army's Advanced Dynamic Spectrum Reconnaissance (ADSR) offers novel technology to help avoid enemy jamming and reflects importance of military engagement with academia and high-tech startups on emerging technologies (<u>source</u> and <u>source</u>)

Assessment: In November, the US Army revealed that it has tested the new Alenabled ADSR tool to support electronic warfare missions. The technology allows the Army's wireless communications networks to sense threats and adapt to communicate on other frequencies in which adversaries are not operating. It can also lessen radio frequency transmissions, reducing risks of adversary force detection of communications. The tool was recently deployed by an electronic warfare unit during a multi-national exercise in Germany. US Army Cyber-warfare officer Brenden Shutt noted that ADSR "sensing capabilities that provide a real-time understanding of the spectrum" are critical to maintaining "dominance in electronic warfare." The AI-driven solution was developed by Vanderbilt University and "has been continuously refined since 2021", according to an Army press-release, demonstrating the importance of militaries establishing mechanisms to better engage academia, applied research, and high-tech startups performing research on cutting edge technologies. Adam Jay Harrison, Vanderbilt Distinguished Entrepreneur in Residence and ASDR team member, assessed that "the technologies [that were] leveraged for the ADSR effort would likely have never seen the light of day were it not for [the Army's] Pathfinder" program, which is designed to increase collaboration between the Army and academia on specialized operational problems.





2. Autonomous systems and robots

2.1 Beep, beep: Roadrunner anti-air drone introduced

On 6 December, Anduril Industries revealed a small operator supervised autonomous drone that can hunt for and destroy enemy drones (<u>source</u>, <u>source</u>, and <u>source</u>)

Assessment: Anduril's system is another novel counter-drone approach designed to more effectively and inexpensively meet the mounting threat from drones and drone swarms that have prominently featured in recent conflicts, including in Ukraine. The Roadrunner is an autonomous vertical take-off and landing drone that can reach high subsonic speeds using its twin turbojet engines. It is capable of loitering and searching for aerial threats before moving to intercept those threats. It is also capable of returning to base and reused if no threats have been detected. While Roadrunner can autonomously detect targets, it is operator supervised, meaning that it will not engage any target without human direction. According to Chris Brose, Anduril's Chief Strategy Officer, "our driving belief is that there has to be human agency for identifying and classifying a threat, and there has to be human accountability for any action that gets taken against that threat." Anduril has also developed a high-explosive variant known as the Roadrunner-M, which includes faster launch and take-off timing, three times the warhead payload capacity, ten times the one-way effective range, and is three times more manoeuvrable." Both Roadrunner variants are stored in an automated hangar known as the "Nest" for transport, maintenance, and launch, which includes a system health monitoring capability to ensure the system is able to respond to imminent or emerging threats.



Figures 1 &2: Left: The Roadrunner-M system. Right: The Nest automated hanger for storage, maintenance, health monitoring, and launch. Source: <u>Anduril Industries Roadrunner product page</u>





2.2 Russia employs upgraded Lancet kamikaze drones in Ukraine

Russia is increasing the number and variety of kamikaze drones being used in the Ukraine war as a means to overwhelm Ukrainian air defences at lower cost (<u>source</u>)

<u>Assessment</u>: The Institute of the Study of War's 28 October "Russian Campaign Assessment Report" revealed that Russian forces began using the new Izdeliye-53 kamikaze drone in the Ukraine war on 21 October.

The new drone is upgraded version of Russia's Lancet system, which has been an effective weapon for Russia in recent weeks. The upgraded version "possesses an automatic guidance system than can distinguish types of targets and increase strike success rates." The report also indicated Russian forces have not scaled use of the system as of late October but is testing its effectiveness in "mass synchronized swarm strikes" designed to saturate or overwhelm Ukraine's air defence systems. The report did caution, however, that the Izdeliye-53's payload of 3 to 5 kgs could limit the types of targets it could be used to strike.

In addition to the Izdeliye-53, Russia also reportedly used the Italmas (also known as Izdeliye-54) drone in a recent attack on Kyiv Oblast. The Italmas is described as "<u>a simplified</u> and cheaper version" of the Iranian Shaheed-136, Russia's use of which against civilian infrastructure, in particular, has increased significantly since the start of September. As with the Lancet drones, Italmas is made by ZALA Aero. It uses an internal combustion engine, which provides more range than the Lancet (up to 200 km) and also can be equipped with a larger warhead.



Figure 1: The Italmas drone. source: Military News YouTube channel





2.3 Drones launching drones: Turkish uncrewed ground vehicle (UGV) launches drones in November test, could support swarming operations

Havelsan's Barkan 2 UGV has reportedly been inducted into the Turkish military to facilitate swarm munition attacks. (source)

<u>Assessment:</u> In early November, Turkish company Havelsan announced it had successfully launched reconnaissance and surveillance uncrewed aerial systems as well as a kamikaze drone from the Barkan 2 UGV, marking what it described as a "first in its class" development. The munitions were fired up to 15km at an altitude of 3,000m and had a flight time of 40 minutes. A previous version of the Barkan had demonstrated the capacity to launch missiles earlier this year. The Barkan 2 is a modular UGV that weighs 900 kg—nearly twice that of its Barkan 1 variant—and has a speed of 13 km / hr. It can operate in autonomous or remote-control mode

The *Defence Post* reports that the system has been inducted into the Turkish military and is deployment ready. Current concepts of use appear to revolve around use in swarm attacks. As Veysel Ataoglu, Havelsan product manager, told *Defence Post* that the Barkan 2 would help the Turkish Mixed Swarm Operations Center (KSOM) realize "the concept of using circulating ammunition as a swarm." The ability to use UGVs to iteratively or simultaneously launch multiple loitering munitions in a swarm-style saturation attack offers yet another means of overcoming increasingly sophisticated counter-drone systems and ever-improving layered point air and missile defence systems.



Figure 2: The Barkan 2 UGV launching a kamikaze drone during a recent test. Source: Havelsan





3. Sensors

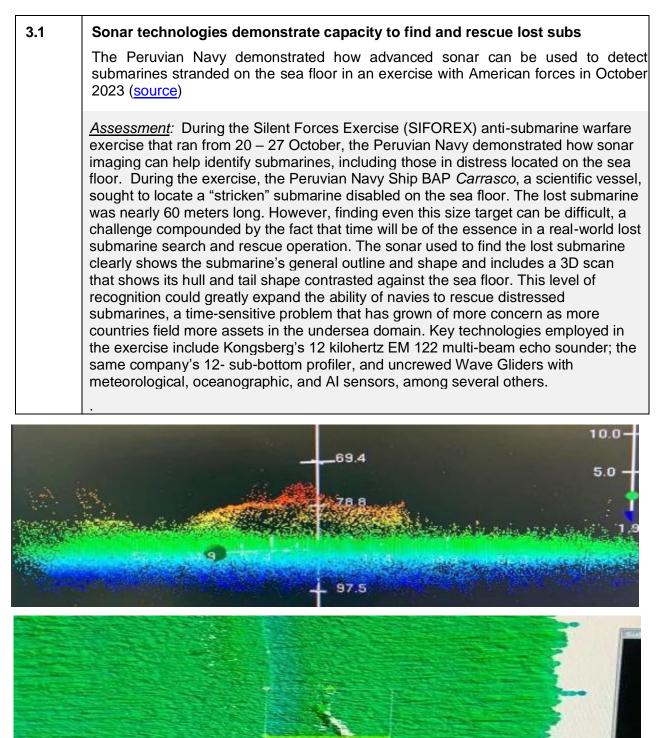


Figure 3: Images taken of the "lost" submarine on the sea floor by BAP Carrasco during the SIFOREX exercise held in late October. Source: Peruvian Navy





3.2	Diamonds are a radar's best friend: New man-made diamond coated chip could solve heat challenges for gallium nitride chips DARPA program hints at innovations that could deliver smaller, more powerful radars
	<u>Assessment</u> : The US Defense Advanced Research Projects Agency (DARPA) is working with Raytheon to develop extra-cool gallium nitride (GaN) semiconductors as part of its Technologies for Heat Removal at the Device Scale (THREADS) program.
	One of the main challenges with radar design and performance is devising ways to manage the temperature of the supporting electronics. Raytheon is seeking to integrate diamond crystals grown onto chips with help of partners Diamond Foundry and Stanford University, a process that has been supported by recent breakthroughs in nanotechnology and lab-ground diamonds.
	Diamonds are excellent thermal conductor. Matt Tych, Raytheon's Mission Area Director for Next-Generation Sensors and Microelectronics, told <i>Defense One</i> that "in terms of comparing thermal performance, today's silicon carbine substrates have a conductivity of about 300 [Watts per meter-Kelvin]. The diamond is 2,000."
	GaN semiconductors are being used in modern radar systems and provide these systems with increased power of emissions that reflect off incoming threats. By improving the cooling capacity of these already powerful chips and introducing new semiconductor architectures, DARPA hopes to create even smaller and more powerful radar and sensing capabilities that will, in turn, allow for more autonomous recognition of environments by drones and planes and improved situational awareness for the operator.





4. Connectivity

4.1	Don't believe your lying eyes: Deepfake detection and the academy An article published in the journal <i>Scientific Reports</i> details research on understanding the vulnerabilities of education stakeholders to science deepfakes and the characteristics that moderate vulnerability (<u>source</u>)
	<u>Assessment</u> : Misinformation and disinformation on important scientific, technology, and science and technology policy issues have become more sophisticated and prevalent with intensifying and worrying effects for academia and society. It is also worrying for national security communities both because debates over scientific issues such as vaccines, climate change or others can amplify existing societal and geopolitical tensions or create new ones that have widespread implications for defence and security communities. One operational example, disinformation around Covid vaccinations led to some military personnel choosing to refuse vaccine mandates creating staffing and readiness challenges. At a more strategic level, deepfakes, including those about scientific issues, have been used to affect the unity of states and societies, which can in-turn reduce options for crisis deterrence or response.
	As a result, it is important not only for academia, but also national security communities, to understand the ways in which the scientific and education community is vulnerable to deliberately altered videos and photos and whether there are broader lessons about vulnerability to deepfakes more generally that can be determined from an examination of the academic community.
	An interesting recent study from researchers at the RAND Corporation, Carnegie Mellon University, Pardee RAND Graduate School, and the Challenger Center addresses this topic by examining the three study questions below for individuals from five populations—K-12 students, higher education students, teachers, principals, and general adult learners.
	 What is the effect of receiving a deepfake video on an individual's ability to correctly identify a video's authenticity and how does that effect vary by population?
	• What characteristics of the video do respondents analyse to determine the authenticity of the video and how are they related to the probability of correctly identifying the video's authenticity?
	• How does the effect of a deepfake video on an individual's ability to correctly identify a video's authenticity vary by respondent background and beliefs?
	Some key study findings include: 1) 27-50% of all individuals surveyed could not distinguish authentic videos from deepfakes; 2) All surveyed populations demonstrate vulnerability to deepfakes, but this vulnerability increases with age and trust in information; 3) adults and educators exhibit greater vulnerability compared to students; and 4) vulnerability increases with exposure to potential deepfakes, meaning that active intervention is required to stem the pernicious effects of deepfake consumption.





4.2 Hacked drone feed leads to Ukrainian strike on Russian drone base

The incident demonstrates the increasing importance of secure communications, data security, and the cyber domain and electromagnetic spectrum in modern conflict (source with video embedded)

<u>Assessment:</u> In late November, Ukrainian forces intercepted the feed of a Russian first-person view (FPV) drone operating in Kherson. Captured footage was then sent to Ukraine's 36th Marine Brigade, which geolocated the data and sent a reconnaissance drone to investigate, according to Ukrainian drone commander Robert Brovdi. Further reconnaissance of the geolocated base showed signs, such as visible antenna and cables running into a specific building, that the base was controlling Russian FPVs. Video posted on the Birds of Magyar X account show the operation unfolding including Ukrainian fires striking and destroying the building in question. The incident reinforces a key theme of previous reports: the intensity of the competition and conflict in the cyber domain and in the electromagnetic spectrum and how carelessness on one side and creativity on another can lead to real tactically, operationally, or even strategically relevant consequences.





Figure 6: Screen shots of a video of the Ukrainian armed forces attack on a drone base in Krynky. The image on the left identifies the building that was ultimately targeted and struck. The image on the right shows some of the evidence collected by Ukrainian drones on the base and its activities. The video from which these images were taken also shows the strike against the building suspected of running FPV drone operations against Ukraine. Source: <u>Special Kherson Cat X account and Business Insider</u>





5. New Weapons

5.1	Architecting the fleet of the future
	Changing requirements and emerging technology are altering the processes and concepts involved in the design and manufacture of modern naval vessels according to the article "Re-Balancing Design: New Technology and Thinking in Naval Architecture" by Dr. Lee Willett, which appeared in the November issue of <i>Asian Military Review</i> (source)
	<u>Assessment</u> : The article explores how naval architecture—the practice of designing vessels to meet current and emerging requirements, especially as it regards ship safety, ship performance, and ship geometry—has changed in the "contemporary environment."
	This environment is characterised by emerging threats that are driving new operational requirements as well as new technologies that is "both driving the threat and enabling the operational response."
	The article focuses on several specific technology, capability, and requirement drivers of changes in approach to naval vessel design:
	First, digital engineering has allowed for testing can be done "more extensively and exhaustively." According to one designer interviewed for the article, "we now want to explore more, so instead of doing five options, we want to do 100 we're seeing our ability to model and integrate things in more complexity grow." This provides exceptional value at several stages of design and manufacture, but especially during the design phase in which "rather than looking at a small number of hullform iterations, you can now explore a huge variation."
	The article also explores how digitisation and AI have allowed designers to not just better model designs but also the nature of the threat that ships must be designed to meet and endure, One naval designer suggested that his team is more focused today on balancing three aspects of resilience and survivability against dynamic threats: susceptibility to detection; ability to survive damage; and recoverability.
	The author also explores the need for flexibility, including distinguishing between design concepts such as adaptability and modularity, each of which brings trade-offs and compromises that must be balanced against mission needs.
	Designers now must also account for the incorporation of more uncrewed systems and AI / ML systems, which changes how humans interact with the ship and even how many humans will be on future naval vessels as both uncrewed systems and machine learning algorithms take over tasks that are too dull, repetitive, or dangerous for humans to carry out.
	Achieving this balance in design and concept of how best to integrate new AI-driven capabilities with the need to have some degree of operator control of decision-making and mission management is a huge component of the evolving ship design process.
	As, Jake Rigby, one of the ship designers interviewed for the piece observed, "the challenge is that, in naval architecture, there's never an optimized solution. You can never say,' I've got a fully optimised hullform' because it's a balance, a compromise. The human in the loop is providing that assessment of what the better compromise is, and that's not something—even with machine learning and other tools—that you can [otherwise] really make."





5.2 Edge Group reveals massive, flexible testing facility in UAE

The site is the first of its kind and size in the region and can support a wide range of testing activities. It will become available to international customers in 2024, further demonstrating Edge Group's growing capabilities and prominence in the regional and global defence industry (company press release and additional source)

<u>Assessment</u>: On 13 November, the first day of the Dubai Air Show, Emirate defence conglomerate Edge Group announced the launch of X Range, the first international defence, aerospace, and commercial products testing, evaluation, and training ground in the region.

The range sits on a secure island known as Abu Al Abyad, about an hour's drive from Abu Dhabi, which is 350 square km. The facility is designed to be able to test a wide range of military and commercial platforms, systems, and technologies and will include: A 3,800m runway for large aircraft, a 1,200m runway for uncrewed aircraft, an urban training village for special operations and law enforcement training; an island-wide communications network; a dedicated shoreline on the north of the island for amphibious operations testing and training, a directed-energy weapons testing area as well as capabilities to test other electronic warfare systems. While to date, the site has been used only to test Edge Group equipment, the expectation is that it will become available for international customer use in 2024.

The announcement of the facility reflects the persistent market for and importance of real-world testing of weapons systems and training even in a world in which a large amount of testing and training can be done in the virtual world. It also offers more insight into the increasing capacity and visibility of Edge Group in the regional and broader international defence market. Edge has positioned itself as a rapidly developing local and international supplier and has also expanded its international portfolio through acquisitions of several foreign defence industry firms, including MilRem Robotics, the Estonian manufacturer of the widely used THeMIS modular uncrewed ground vehicle, among others.



Figure 7: A rendering of Edge Group's X-Range. source: Edge Group press release





6. Space

6.1	North and South Korea launch first ever military spy satellites
	Moves demonstrate the importance and sensitivity of military activity related to the space domain and raises questions over Russian technological support for North Korean space and military programs (<u>source</u> , <u>source</u> , <u>source</u> , <u>source</u>)
	<u>Assessment</u> : On 21 November, North Korean state media claimed that the country had successfully launched its first ever military spy satellite—the Malligyong-1—into orbit. The launch came after two failed attempts earlier in the year.
	Officials in South Korea and Japan acknowledged the launch and that the satellite was placed into orbit but withheld any statements about whether the system was functioning properly.
	Subsequent statements from the North Korean government have claimed that the satellite has transmitted imagery of: the White House and Pentagon in Washington, D.C., U.S. aircraft carriers at a navy base and a shipyard in Virginia, U.S. military facilities in Guam and Hawaii, and key sites in South Korea. Many experts remain sceptical that these claims are accurate or that the system is sophisticated enough to function as an operational spy satellite.
	Despite this scepticism, the United States, Japan, and South Korea immediately condemned the launch as being provocative and contravening several U.N. Security Council resolutions banning North Korean satellite launches. These launches are viewed as covers for development and testing of long-range missile technology.
	Development and successful launching of spy satellites has been a priority of North Korean leader Kim Jong Un. Sources in South Korea reportedly believe that North Korea was able to pull off the successful test only with technological assistance from Russia, citing the September meeting between Kim Jong Un and Vladimir Putin at the Vostochny space centre. Many observers believe a deal was reached during this meeting North Korea to send Russia arms for use in Ukraine in return for technical assistance in satellite and other military capabilities.
	Other analysts note that the time between the meeting in Russia's Far East and the satellite launch was possibly insufficient for this assistance to have been effectively provided and that, as Ankit Panda of the Carnegie Endowment observed, " <u>this was</u> <u>North Korea's third launch attempt and they've been carrying out their own</u> <u>research and development on space systems for a while.</u> "
	Regardless of the scale and importance of Russian support, the launch has increased tension on the Korean Peninsula and contributed to South Korea launching <i>its</i> first ever military spy satellite on 1 December from Vandenberg Space Force Base in the United States. It was the first of five spy satellites South Korea intends to launch by 2025, all of which will use SpaceX's Falcon 9 rocket.





6.2	Project Nyx Alpha to provide increased space domain awareness for UK MoD New program reflects the criticality of coordinated military / commercial space domain awareness in managing and protecting space assets critical for national security, defence, economic activity, and commercial communications and navigation
	<u>Assessment</u> : On 22 November, the UK Ministry of Defence announced it had signed a contract with a small London-based company named SpaceFlux to establish and operate a ground-based telescope in Cyprus by the spring of 2024.
	"Project Nyx Alpha's" main objective is to allow the UK Space Command and UK Space Agency to accurately monitor the increasing number of satellites and debris in low earth orbit (LEO), geostationary orbit, and in cislunar space. The effort will coordinate both military and commercial / civil – focused space domain awareness activities and, ultimately, to help the UK defend its interests in space.
	According to Air Vice-Marshal Paul Godfrey, head of the UK Space Command, "space domain awareness underpins our ability to protect and defend UK and allied interests in space. The UK has critical assets in geostationary orbit, and Project Nyx Alpha will help us to monitor them more closely."
	The facility will be built on Cyprus due to the fact that the country provides a better view of the geostationary orbit than sites on the UK mainland. In addition, the UK already has a major military base on the island.

6.3	China's reusable space plane places six "wingman" objects into space orbit
	Some of the small objects appear to be transmitting as part of a more sophisticated test of the plane's capabilities than in even the recent past. The timing of the plane's mission aligns closely with the launch of a mission of the US X-37B spaceplane later in the month (<u>source</u> and <u>source</u> and <u>source</u>)
	<u>Assessment:</u> On 18 December, China's reusable space plane known as Shenlong "Divine Dragon", which had launched on 14 December, reportedly placed six objects into earth orbit. The nature and function of these objects is not known, though, amateur space watchers have tracked their orbits and transmissions closely and compiled compelling evidence that the objects were placed in orbit by the Shenlong. The objects have been named Objects A, B, C, D, E, and F. Amateur spacecraft tracker Scott Tilley told <i>Space.com</i> that Object A appears to be emitting signals reminiscent of those emitted by objects that China's space plane has released on previous missions while Objects D and E appear to be emitting idle "placeholder" signals with no data accompanying them. While the spaceplane has placed individual items into orbit in the past, this experiment is not only large in scale, the items that are emitting are "operationally exhibiting different radio behaviour than before", perhaps signalling that the Shenlong program has matured to the point at which more sophisticated tests are possible, <u>according to <i>The Drive</i>.</u>
	The closely watched launch of the Shenlong comes only two weeks before the United States is scheduled to launch its own reusable spaceplane—the X-37B—currently scheduled for 28 December. The X-37B was originally scheduled to be launched on 11 December, but the launch was abruptly scrubbed, leading some to speculate that the hurriedly scheduled Chinese launch for three days later could have interfered with US plans.

https://deftech.ch/