Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

DEFTECH-SCAN

November 2026

deftech.ch

OTH INTELLIGENCE GROUP

ladf.online/d-scan

Dear Reader,

We welcome you to the October & November 2026 edition of the Deftech Scan.

This edition is entitled ***Integration.*** Across the stories in this volume, AI, data, sensors, robotics and commercial services are being integrated into connected military capabilities. Yet this integration is neither frictionless nor uniform. Budgets, industrial models, trust, visibility and the specific demands of individual theatres continue to shape how quickly, and in what form, these capabilities emerge. The stories in this report examine both the direction of travel of integration and the constraints that will determine its pace.

Key themes from this report include:

- **Connected capability: from sensing to deciding to acting:**
  Militaries are working to link AI, data, sensors and uncrewed platforms into a single connected capability meant to detect, discern and prioritise threats, decide how best to manage them, and respond more quickly and precisely. South Korea's proposed 2027 budget would raise planned spending on AI and crewed-uncrewed systems by 55.5 percent, alongside a cloud-based system to connect data across fragmented command-and-control networks. The UK–Ukraine AI partnership opens battlefield data from Ukraine's Avengers AI Labs to British researchers, while private Chinese firms are building Palantir-style data-fusion and decision-support platforms for the PLA. The emerging competition, then, is one to accelerate integration of sensing, training data, sense-making and recommendation capabilities, and decision-making.

- **Military and commercial convergence as an amplifier and vulnerability:**
  Commercial companies are now central to military capability. This is true in software and AI development, but it is also highly relevant to the space domain, as reflected in the five space-related stories in this volume across multiple categories. Indeed, a central theme of the U.S. Defense Intelligence Agency's (DIA) *Challenges to Security in Space* is that commercial space has now become a valuable component of national security and military communications and sensing activities. The same dependence creates new vulnerabilities. SpaceX's ten-day restriction of Ukraine's Starshield access showed that critical services can hinge on decisions beyond a military's control while Russia's close approach to an ICEYE radar satellite showed that commercial spacecraft are becoming targets of strategic pressure.

- **Building the architecture, not just the platform:**
  Several stories suggest that efforts to optimise the value of new systems increasingly lie in building the tools and supporting capabilities and architecture to enable them. The U.S.–UK launch of a Mk 48 torpedo from the XV *Excalibur* XLUUV is an important milestone but is perhaps more notable for the tricky integration of mechanical, electrical and software elements of the test to employ an allied weapon from an autonomous platform. China's apparent second UUV mothership reinforces this point. As China builds out its extra-large uncrewed underwater vehicle fleet, such motherships will allow these new and highly capable platforms to operate outside of the First Island Chain and further from home. Additionally, collaborative combat aircraft are increasingly becoming defined by the software that enables autonomy and mission management as much as by the airframe, an insight visible in the focus on sovereign software development consistent across the approaches to CCA development of both Germany and France.

- **Robots as substitutes, not just tools:**
  The vision for the future of the development of uncrewed systems is expanding and this report highlights how at least two militaries around the world are thinking of these systems. A former Ukrainian Defence Minister proposed an Army of Robots for Ukraine in which humanoid and other types of robots are deployed essentially to replace human infantry, carrying out dangerous battlefield combat tasks while humans wait for a safer environment to advance forward and take territory. South Korea's increased focus on AI and uncrewed systems emphasizes human-machine teaming as a way to amplify human activity and keep humans out of harm's way when possible as a means of compensating for a sizable reduction in the size of its armed forces over the last two decades.

- **Integration and constraints:**
  Integration is the main trend of this volume. However, constraints and limitations to and trade-offs associated with this integration remain. They will determine the pace and shape of integration efforts, and actors are already responding to them in different ways. Europe's collaborative combat aircraft efforts show the divergence. France is building a sovereign AI test bed on converted Mirage 2000s, while Airbus is partnering with Kratos on a more mature airframe, each trading off control, cost and speed. SOUTHCOM is seeking systems "uniquely tailored" to its rivers and jungle rather than more generic systems. Additionally, the reporting on China's UUV motherships and massive WZ-X drone remains largely inference from satellite imagery rather than firm statements of capability, mission, and intent while Chinese analysts acknowledge that the PLA's gap in developing AI-enabled decision-support systems lies less in technology than in overcoming bureaucratic challenges in applying it.

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

1. **Applications of AI and data** **3**
2. **Robotics and Autonomous Systems** **6**
3. **Connectivity** **13**
4. **Platforms and Weapons Systems** **17**
5. **Space** **20**

We wish you an interesting read.

Foresightly Yours,



Tate Nurkin
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	**Republic of Korea's (ROK) connected-force push: South Korea moves AI, crewed-uncrewed teaming, and counter-drone systems up its defence agenda** South Korea's proposed 2027 defence budget of KRW 73.27 trillion (USD54.6 billion), up 8.2 percent from 2026, would increase planned spending on AI and crewed-uncrewed systems by 55.5 percent and on drone and counter-drone capabilities by 18.8 percent. The push aims to link AI, uncrewed platforms, sensors, and command networks into a connected force. (source, source, and source) *Assessment:* Two companion *Asian Military Review* (*AMR)* articles published on 9 October tie the investment to government priorities announced in an Armed Forces Day address on 1 October. The address called for accelerating AI-enabled command and control, high-energy laser interceptors, and other future capabilities. South Korea is continuing investment in unmanned ground surveillance sensors, explosive-ordnance detection and disposal robots, autonomous mine-countermeasure systems and other platforms designed to reduce personnel exposure to dangerous missions and amplify the impact of the country's armed forces through human-machine teaming. The articles highlight multiple examples of current activities, with one article referencing a new KRW 43 billion (USD31.9 million) demonstration program for AI-enabled physical systems in areas such as transportation, base security, and hazardous-material handling. A second example is the 6 October announcement from the Defence Acquisition Program Administration (DAPA) of a program for a cloud-based Command and Control Information Sharing System. The project is meant to connect data, services, and terminals currently spread across joint and service-level command, control, communications, and computer and intelligence (C4I) networks, providing a digital backbone for faster information sharing and decision-making across units. Both articles emphasize that these technology priorities will also feature at the K-DEX 2026 defence exhibition, scheduled for 8–11 December in Goyang. The agenda for the event is built around at least four core themes that align with the government agenda announced on 1 October: Autonomous systems and crewed-uncrewed teaming, intelligent command and control, precision strike, and drone and counter-drone technologies. The push for increased AI adoption is, of course, rooted in part in the growing impact that AI and uncrewed systems are having on a broad range of military operations, especially AI's role in support of improving and accelerating situational awareness and decision-making. However, it is also worth noting that AI and uncrewed systems investments will also help address an urgent manpower crisis within the RoK armed forces. Since the early 2000s the size of South Korea's military has dropped from 690,000 to about 450,000 today, the result of historically low birth rates and a drop of the number of 20-year-old men by 30% from 2019 to 2025.

1.2	**Enabling the enablers: Data sharing at the centre of UK–Ukraine AI partnership** The United Kingdom and Ukraine announced an AI partnership on 24 August that gives British researchers and companies access to data from Ukraine's Avengers AI Labs to train British national security AI models. The agreement reflects the criticality of current tactical and operational battlefield data to training military and security AI algorithms. It also reinforces the changing nature of collaboration between Ukraine and its European partners. (source and source) *Assessment:* The agreement seeks to leverage Ukraine's battlefield experience in combination with the ecosystem of UK universities, researchers, and technology firms. In announcing the deal, UK Prime Minister Andy Burnham focused on the deal's value for UK infrastructure protection, observing that "by combining Ukrainian battlefield data with British expertise, we will accelerate the development of capabilities that not only strengthen our national security but better protect our critical infrastructure and growth in every postcode here at home." Avengers draws on thousands of daylight cameras and infrared sensors that have recorded objects including tanks, artillery, air-defence systems, infantry, and drones. For the UK, the agreement offers a promising potential pathway to develop novel capabilities on a data set that is proven in conflict and to collaborate with individuals who have used technology under fire and in highly contested situations. For its part, Ukraine gains access to, according to the British government's press release, "world-leading universities, researchers, technology companies and third largest AI eco-system in the world, allowing Ukraine to draw on British expertise to accelerate the development of solutions to urgent challenges." The UK announced pilot projects involving three British startups: • Sintela, a fibre-optic sensing and infrastructure security company specializing in distributed acoustic sensing; • Mind Foundry, an Oxford University machine learning and sovereign AI spin-out focused on building responsible AI for high-stakes domains; • Skyral, a modelling, simulation, and digital twin software firm building scalable synthetic and digital environments. The first pilot is preparing to test technology at a UK defence site that uses buried fibre-optic cables as AI-enabled sensors to detect activity around the base. The second pilot effort will explore low-power AI chips for drones, robotics, and autonomous systems. Additionally, as with the Germany–Ukraine joint production model discussed in the August DEFTECH Scan, the arrangement reflects the broader shift away from donor-recipient models between European countries and Ukraine toward leveraging Ukraine's battlefield innovation, manufacturing scale and resilience, and proven capabilities for mutual research, development, and production of critical capabilities and weapons systems.

1.3	**Palantir with Chinese characteristics? Private software firms joining efforts to "intelligentise" People's Liberation Army (PLA) military operations** The number of private Chinese technology firms working with China's defence and security communities has increased in recent months and years as part of intensifying efforts to develop and adopt AI-enabled data fusion and decision-support platforms across PLA operations. However, several analysts argue that the primary challenge facing the PLA is its ability to integrate, trust, and operationalize AI at scale. (source) *Assessment:* An August *South China Morning Post* report examines how China's military-civil fusion strategy (MCF), which stresses the integration of private sector technology development for national security purposes, is increasingly being applied to software, data, and decision-support activities. These capabilities are viewed as critical to future military effectiveness and to the "intelligentisation" of conflict that the PLA is trying to achieve. As retired PLA colonel and defence analyst Yue Gang observed in the article, "in traditional warfare, the observe-orient-decide-act (OODA) loop is measured in hours or even days. However, in modern conflicts, AI-assisted systems can compress this cycle to just seconds. Data fusion, situational awareness and decision support represent the strategic high ground of future military competition." The increased number of commercial software firms working with the PLA is not dissimilar to a similar trend in the United States and Europe, where software-focused defence firms have become influential parts of the broader defence technology and industrial base. Companies such as Palantir have demonstrated the value of software platforms that integrate information from multiple sensors, databases, and operational systems into a common operating picture. Rather than simply employing artificial intelligence, these software providers seek to become the connective software layer integrating data collection, analysis, planning, and operational execution. According to the article, "hundreds" of private technology companies are reportedly involved in defence-related AI projects spanning data fusion, autonomous systems, battlefield simulation, and AI-assisted training. Among the most prominent new entrants is Jingan Technology, whose Jingqi Global Situational Awareness System combines satellite imagery, sensor feeds, and other information streams to support situational awareness, planning, and operational decision-making. The company markets the platform as a domestic counterpart to Palantir's Gotham and Anduril's Lattice systems. Other firms are pursuing adjacent niches, including commercial satellite imagery analysis and AI-enabled military training environments focused on potential Taiwan Strait contingencies. Several analysts have highlighted the challenges China faces in integrating AI-enabled capabilities into military operations. Analyst Hu Bo, director of South China Sea Strategic Situation Probing Initiative (SCSPI), a leading Chinese think tank, argues that "the gap doesn't lie in the technology, but the United States is much further ahead in applying it, particularly in supporting decision-making." Hu and other analysts cite challenges such as duplicated development efforts, limited interoperability among systems, lengthy procurement timelines, bureaucratic barriers to data sharing, and relatively few opportunities to validate AI-enabled concepts under operational conditions as slowing down adoption timelines.

2. Robotics and Autonomous Systems

2.1	**Terminator and other scary and potentially useful things: A vision for ground robots and the future fight** Former Ukrainian Defence Minister Mykhailo Fedorov proposed a "new Manhattan Project" to accelerate the development and deployment of battlefield robots, with the long-term goal of reducing the role of infantry in frontline operations. His proposal is not a current government program. Rather, it is an ambitious vision of a future force structure that reflects the changing nature of ground combat. (source) *Assessment:* Fedorov revealed his plan by showing an AI-generated video of ground robots operating on the front line during the IT Arena show, described as Ukraine's largest technology conference. The video shows different types of robots achieving a range of mostly kinetic missions, including humanoid robots firing weapons, spider-like robots emerging from the ground and exploding in the midst of enemy forces, a canine-like robot running underneath an armoured vehicle before detonating, and an uncrewed ground vehicle defending a fixed position. According to Fedorov, the main objective of his plan is to prioritize the safety of human operators in an environment characterized by near ubiquitous battlefield sensors. Forward deployed robots—autonomous or remote controlled—will carry out dangerous missions and clear the way for humans to more safely enter a combat zone. "We want to eventually substitute our infantry with these robots," Fedorov told *Defense News* in an exclusive interview after the presentation. Fedorov is no longer Defence Minister, so the "Army of Robots" concept is not an official government program. Rather, Fedorov, who recently started a defence company with Palantir CEO Alex Karp, is "calling on specialists in robotics, AI, sensors and autonomous systems to pool their talent in the kind of concentrated wartime push that built the first atomic bomb." The effort's near-term milestones are ambitious and include a "confirmed battlefield result" within six months and, within a year, an assault in which robots handle the most dangerous parts of a mission without infantry alongside them. The model follows Ukraine's Army of Drones initiative, which Fedorov launched in 2022 as Ukraine's digital transformation minister. Army of Drones opened the market to Ukrainian drone makers, launched government procurement and operator training, and helped form the first strike drone units. Unsurprisingly, Ukraine is already a global leader in the use of ground robots, especially in logistics and evacuation missions. Ukrainian armed forces completed more than 25,000 of these missions in August alone, 3.3 times higher than the total number of such missions launched in January, demonstrating the expanding relevance of ground robots to modern conflict.

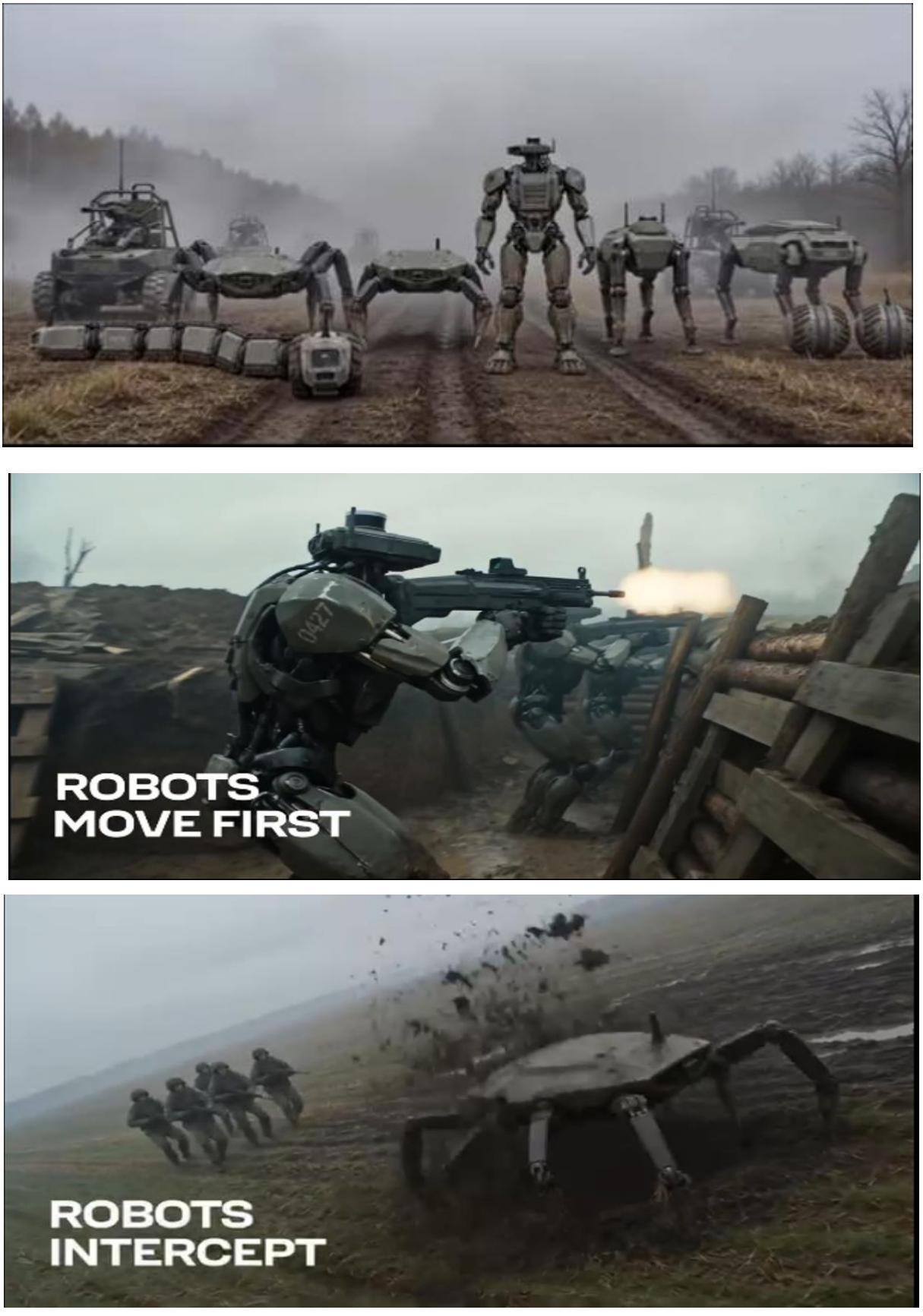


Figure 1: Screen captures from Mykhailo Fedorov's video proposing his Army of Robots concept. Source: Facebook, via Defense News.

2.2	**Sovereign software and Collaborative Combat Aircraft (CCA): Two approaches for ensuring domestic ownership of CCA software enablers** France and Germany are pursuing different industrial approaches to the development of CCA, reinforcing the concept that while CCAs are likely to be at the centre of future tactical air fleets, multiple approaches to development and to retaining ownership of key software capabilities will be pursued. Each approach comes with its own trade-offs, which are especially relevant as European countries seek to meet urgent threats while also building and retaining strategic independence in their respective defence industrial bases. (source, source) Assessment: The August DEFTECH Scan discussed two separate concepts for the role and capabilities of CCAs emerging in Europe with SAAB developing a high-end uncrewed fighter aircraft and BAE focusing more on lower cost, more attritable systems. This volume amplifies and expands the nature of the diversity of industrial model approaches for developing a capability that is increasingly at the centre of future air forces. *Defense News* reported in October that the French Air and Space Force, the Directorate General for Armament, and the Ministerial Agency for Defence AI are converting two Mirage 2000 aircraft into flying laboratories for HypAIRion, France's sovereign CCA initiative. Early experimentation will focus on mission-planning assistance, flight-path optimization, and tactical decision support as France seeks to develop the software, operational concepts, and human-machine relationships necessary for future crewed-uncrewed teaming. The planned 2028 demonstration is intended primarily as a test bed and may not directly produce the future companion aircraft for the Rafale F5. Rather, French officials have emphasized building an open architecture that allows the government to retain control over critical software, data, and autonomy functions while preserving human authority over the use of force. Airbus is pursuing a different path, partnering with American company Kratos to develop the U740 Valkyrie, derived from Kratos' XQ-58A Valkyrie. The companies reported the U740's first European test flight on 29 September, demonstrating basic aircraft performance and in-flight mission modifications. Airbus plans to integrate its MARS mission system during future test flights before progressing toward crewed-uncrewed teaming demonstrations with the Eurofighter. The program aims to deliver an operational capability by the end of the decade, providing Germany and, likely, other European users with a relatively mature air vehicle while preserving European control of mission software and autonomy systems. The two programs reveal a broader discussion emerging within European defence innovation. The question is no longer whether Europe will field multiple types of CCAs, but rather how different countries intend to develop them and control access to the hardware and software on which these systems rely. These are important questions for any capability but are especially so given that CCAs are increasingly becoming software-defined systems whose military value derives as much, if not more, from the autonomy, mission management, and human-machine teaming capabilities they enable as they do from the airframe, hardware, and kinetic payloads they carry.

2.3	**Flying high (and far): New imagery sharpens the view of China's giant WZ-X flying-wing drone** New photographs circulating on Chinese online forums appear to show China's large flying-wing drone, dubbed the WZ-X, in flight, while satellite imagery analysis has confirmed its unusual wing configuration. The system's size and wing design suggest that it is most likely a high-altitude, long endurance (HALE) intelligence, surveillance, and reconnaissance (ISR) aircraft, though the drone's mission, performance, and operational status remain unconfirmed. (source, source) *Assessment:* An in-depth 4 September *TWZ* analysis of the uncrewed system's design focuses on the aircraft's size and unusual wing planform, which offer some insight into the type of mission it is designed to carry out. Imagery from the Malan facility in Xinjiang where the aircraft is being tested shows a broad inner wing transitioning abruptly to long, narrow outer sections, along with a shallowly serrated trailing edge. *TWZ* estimates a wingspan of roughly 170 feet (52 metres), similar in scale to the U.S. B-2 bomber, and assesses that it may have two engines, though these remain estimates rather than published specifications. A long span and narrow outer wing could support efficient high-altitude flight and endurance, while the large centre section could house fuel, sensors, and communications equipment. Andreas Rupprecht, a specialist on Chinese military aviation quoted in reporting from *South China Morning Post,* estimates a range over 12,000 miles and a cruising altitude of 59,000–66,000 feet. While unconfirmed, the range and high operating altitude—making it more survivable—would be consistent with the HALE ISR mission, in short, a platform intended to operate deep inside defended airspace and function as an advanced communications relay node. The aircraft first appeared in satellite imagery (which is published with permission in the *TWZ* article) in May 2025. The new photos that emerged in September clarify its shape and suggest flight testing is progressing, even if there is little confirmed information about its operational status, stealth performance, or role in a combat network. While the aircraft's dimensions and design are innovative, uncertainty remains about the aircraft's capabilities, a point Michael Bosack, director of the Parley Policy Institute, highlighted in comments to *South China Morning Post.* Bosack pointed out that while the size and configuration are receiving considerable attention, "airframes like this are meaningless without the systems they carry." He further noted that "if they can achieve the right flight profile and carry the most useful ISR equipment, then they can stay operationally relevant for decades. Simply put, until we know what sensors or other payloads the Chinese will put into the aircraft, we cannot really determine how useful it will be."



Figure 2: Images of the WZ-X from Chinese internet via South China Morning Post and TWZ. The WZ-X was first seen at China's secretive test base near Malan in Xinjiang province on May 14, 2025.

2.4	**Two sides of the same drone: The drone dilemma in the U.S. Southern Command area of responsibility** Latin American cartels are acquiring battlefield-grade drone skills faster than U.S. and Mexican authorities can counter them, according to an internal U.S. assessment. At the same time, U.S. Southern Command (SOUTHCOM) is building its own uncrewed force to track and disrupt trafficking networks. (source and source) *Assessment:* The drone threat from Latin American cartels is evolving into a more mature capability that includes not only surveillance, evasion and deception, but also a more advanced strike capability, according to an intelligence document viewed by *The Washington Post.* Cartels have studied techniques such as frequency hopping to defeat US and partner jamming efforts while also buying uncrewed aircraft with greater endurance and the capacity to carry larger payloads. Indeed, the intelligence report suggests that at least one cartel possesses aircraft with six to eight propellers, allowing a drone to conduct hours-long flights and carry upward of 150 pounds. Cartels are also acquiring the skills to use these aircraft in more sophisticated and effective ways by recruiting Colombians with combat experience in Ukraine and, US officials allege, sending affiliates to fight there to gain that experience. Retired General Glen D. VanHerck, former commander of US Northern Command and the North American Aerospace Defense Command, warned that the cartels are building the capacity to "use techniques to counter our drones for surveilling them, potentially even attacking them in ways that you would see in the battle space." Use of armed drones in the region is also rising. The Armed Conflict Location & Event Data conflict monitor recorded 38 weaponized drone events in Colombia in 2024, 149 in 2025, and more than 200 by early September 2026. Beyond the cartel drone threat, U.S. SOUTHCOM, which oversees US military operations in Central and South America and the Caribbean, also faces the persistent problem of terrain and how traffickers use rivers to move narcotics and jungle canopies to hide boat-assembly sites. In response, SOUTHCOM commander General Francis Donovan told *Breaking Defense* that he was seeking to establish a "unique river reconnaissance system, representing a tailorable mix of unmanned surface, air and sub surface autonomous platforms." Such systems will be tested and trained on at SOUTHCOM's Autonomous Warfare Command (SAWC). It was established in April 2026 to advance and accelerate the development and adoption of autonomous systems throughout the command and to provide a centre for testing and training, not just on technologies but on operational concepts as well. The key for Donovan is that the autonomous systems that have been developed move beyond testing and demonstrate their value in real-world environments. For example, Donovan noted that Saronic-made Corsair USVs have been moved to Guantanamo Bay, Cuba—a SAWC forward staging and training site—and are also "assisting local forces in narco-terrorist operations and [supporting] the physical security of the [Panama] Canal" on both sides of the canal. Drones and uncrewed systems are at the heart of both the cartels' and SOUTHCOM's operations in the region largely because they offer persistent reach across a vast theatre whose complex and dense terrain enables concealment. The difference in approach, though, is notable and important. Cartel drones are increasingly built and deployed to strike at longer distances and with greater impact while SOUTHCOM's focus area for drone development is in data collection, fusion, and overall domain awareness that can enable interdiction.



Figure 3: A Saronic Corsair uncrewed surface vehicle

3. Connectivity

3.1	**Pushing the spectrum fight forward: France considers non-specialist EW platoons to support manoeuvre forces** The French Army is considering non-specialist electronic-warfare (EW) platoons that would operate dismounted near the front line to detect, identify, locate, and share electromagnetic targets in support of manoeuvre forces. Drawing on lessons from Ukraine, the proposal suggests France increasingly sees the spectrum as a tactical problem to be fought at the point of contact, rather than one left mainly to specialist units in the rear. (source) *Assessment:* A 6 July *Armada International* article, citing sources close to the Armée de Terre's (ADT/French Army's) Electronic Warfare (EW) units, reports that a "major change is planned for the force's EW order-of-battle" in which non-specialist EW platoons would be activated. *Armada* stipulates that the exact configuration and number of these platoons is yet to be determined but that they will be dismounted and will be established to detect, identify, locate and share electromagnetic targets across a waveband of around 500 megahertz/MHz to six gigahertz/GHz. Specific targets are likely to include drone control and video links, tactical radios, cellular networks, radio-controlled improvised explosive devices, and satellite-navigation signals. The rationale for the move is to make the force as survivable and operationally flexible as possible. In Ukraine, large EW vehicles operating near the line of contact have proven easy to spot, with antenna arrays that betray their purpose. They are also vulnerable to drone-delivered munitions and one-way attack drones. Dismounted teams, by contrast, have achieved significant effects while staying mobile and dispersed. The result of this doctrinal shift would be a layered structure in which forward platoons would fight for local electromagnetic superiority while heavier specialist units further back, built around the Serval-GE vehicle delivered since August 2025, would manage the wider spectrum battle and analyse complex or unfamiliar signals passed back by the platoons. Two challenges stand out. First, putting collection and jamming equipment in the hands of non-specialists raises training and deconfliction questions, not least the risk of jamming friendly drones and radios in a crowded spectrum. Second, the plan is not settled. The number and size of the platoons, and whether they will belong to specific brigades, remain undecided. Even so, the proposal signals a significant shift, moving EW from a supporting technical speciality towards a core part of combat power that is more fully integrated into manoeuvre operations.





Figure 4: Top: Several of the Thales systems that could equip the French Army's proposed non-specialist EW platoons were on display at this year's Eurosatory exhibition held in Paris between 15th and 19th June. Source: Armada International and Bottom: The French Army is taking delivery of the KNDS VBMR-L Serval-GE electronic warfare platform which will support tactical- and operational-level EW for the manoeuvre force. Source: Armada International

3.2	**Trust, once questioned . . . : Starshield disruption highlights the risks of military dependence on commercial networks** SpaceX restricted Ukraine's use of its military-grade Starshield network for ten days from 14-24 October, cutting the connection to drones flying faster than 100 mph (160 km/h) during intensified Russian missile and drone attacks. Ukrainian President Volodymyr Zelenskyy pointed to the decision's tragic consequences, saying that "people were killed because [there was] not enough destruction, not enough interceptors, including interceptors with Starlink, which didn't work, of course." (source and source) *Assessment:* The decision caused a range of reactions and a heightened degree of concern about relying on any single provider of communication capability, especially one controlled by individuals that may have their own geopolitical and political objectives and who may not be accountable to the governments they support. SpaceX CEO Elon Musk initially said speed limits were set by the U.S. military and ultimately the president. However, he later acknowledged that SpaceX had imposed the restriction, claiming Ukraine had violated Starlink's terms of service by using the infrastructure for offensive strikes, an accusation Kyiv denies. U.S. senators expressed concern about the decision and authored a letter asking SpaceX to answer a series of questions about the decision. A second letter was sent to U.S. Secretary of Defense Pete Hegseth questioning the reasons behind the outage and urging Hegseth to take action to ensure Ukraine's persistent access to Starlink. German Foreign Minister Johann Wadephul—Germany funds Ukraine's Starlink access—made a statement in which he noted that his country expects the service to work because it is paying for it. Full service returned on 24 October, a day after U.S. President Donald Trump reportedly asked Musk to lift the restrictions. Beyond the operational and human impact, the decision revealed a massive vulnerability for Ukraine, one that could also be felt by other militaries relying on Starlink or, really, any commercial provider. Military planners need confidence in their kill chains, and this episode showed that access can hinge on decisions and disputes beyond their control. History suggests the decision could also have unintended consequences for the U.S. space industry beyond SpaceX, which is likely to face increased competition from new providers in the mid-term. For example, India was denied GPS access during the 1999 Kargil conflict and responded by building its own navigation system. Similarly, also in 1999, Europe began pursuing Galileo, which became operational in 2016, demonstrating how unreliable access can push partners to seek additional capabilities, including sovereign ones. Ukraine is already moving to diversify its suppliers, having signed a development agreement with Denmark's GomSpace in April. Additionally, on 22 October, it signed a letter of intent with ICEYE and Nokia for sovereign satellite communications. However, the short-term challenge is that none of these systems can replace Starlink soon, creating a lingering dependence and vulnerability even if the mid-to-long term likelihood of multiple proliferated communications constellations across various orbits will create strategic flexibility.

3.3	**More than one a day: Cyberattacks on the space sector hit the ground, but activity in orbit may simply go unseen** A report entitled “Space Cyber Threat Intelligence: Threat Landscape Report 2025” from Clemence Poirier at ETH Zurich’s Center for Security Studies identified 407 cyber incidents affecting at least 183 space-related organisations in 46 countries during 2025. Interestingly, none of these incidents could be confirmed as targeting satellites in orbit. The report refers to the absence of verified attacks against in orbit assets as a “blind spot” rather than a verification of the security of satellites on orbit from cyber-attacks. (source) *Assessment:* The incidents documented in the 30 September report involved 139 threat actors, predominantly hacktivist groups. Distributed-denial-of-service attacks accounted for 61 percent of the activity, followed by ransomware at 13 percent, with data breaches and leaks making up much of the remainder. Perhaps unsurprisingly, the focus and timing of this threat activity tracked closely with geopolitical flashpoints as politically motivated groups targeted the space sectors of their perceived adversaries, with spikes in attacks coinciding with the war in Ukraine, the Israel-Iran war, the conflict in Gaza, and tensions between India and Pakistan. Significantly, the report documents not only the number of incidents and threat actors but also stresses the importance of understanding where they occurred. The documented attacks targeted ground infrastructure, operators, suppliers, user terminals, and enterprise IT networks rather than satellites in orbit. While these numbers do reflect the vulnerability of the ground component of space infrastructure, the absence of data on attacks on satellites in orbit should not be interpreted as evidence that satellites are inherently secure. Instead, it highlights a fundamental data and transparency challenge. Most operational satellites carry limited cyber-monitoring capabilities, meaning hostile activity in orbit may generate few observable indicators. The count is also uncertain in the other direction, since hacktivists frequently exaggerate or fabricate claims while victims often remain silent. As a result, the 407 incidents should be understood as a record of what the research was able to identify and verify through open sources, not necessarily a comprehensive accounting of cyber activity affecting space systems. The author attributes this visibility gap to fragmented threat intelligence, inconsistent definitions of what constitutes the space sector, limited reporting, and the difficulty of applying conventional cyber-intelligence methods to space systems. At the same time, trends such as commercialisation, digitalisation, growing use of commercial off-the-shelf technologies, and greater technical transparency are eroding the sector’s traditional reliance on security through obscurity. Attackers are learning more about how space systems work, while defenders still struggle to generate and share comparable awareness. Therefore, the report argues for a shift towards security through transparency, including improved onboard detection capabilities, common terminology, space-specific threat frameworks and more systematic information sharing. The recommendation reflects a broader reality that space cybersecurity is not solely a satellite problem but an enterprise challenge spanning spacecraft, ground stations, operators, suppliers, and supporting networks, many of which are increasingly commercial in nature.

4. Platforms and Weapons Systems

4.1	**First shot from an uncrewed submarine: U.S. and UK test a torpedo launch from the XV *Excalibur*** The U.S. Navy and UK Royal Navy launched a U.S. Mk 48 heavyweight torpedo from XV *Excalibur*, Britain's 12-metre, 19-tonne XLUUV on 13 September in a first-of-its-kind test conducted under AUKUS Pillar II. The demonstration marks an important step toward integrating allied weapons and autonomous platforms, though it remains an early proof of concept . (source, source, and source) *Assessment:* The trial took place at the British Underwater Test and Evaluation Centre in Scotland under the U.S. Navy's Project Broadsword and the Royal Navy's Trial Iron. While the launch was considered “historic”, the key challenge was in achieving the integration required to make it possible. *Excalibur* carried a specialized management system capable of controlling and releasing a U.S. Mk 48 torpedo from an allied autonomous platform. Because the heavyweight torpedo could not fit inside the vehicle's payload bay, it was mounted externally. The U.S. Navy stated that the trial validated the "mechanical, electrical, and software integration" necessary to employ a U.S. kinetic payload from an autonomous allied vessel. The project progressed from approval to testing in less than seven months. The demonstration represents an important milestone for AUKUS efforts to accelerate technology integration and interoperability among partner nations. Rather than focusing solely on developing new platforms, the trial showed how allied weapons, software, and autonomous systems can be combined rapidly to produce new capabilities. At the same time, the test leaves many operational questions unanswered. The Royal Navy later clarified that the trial employed an inert, recoverable torpedo and formed part of a broader three-week experimental campaign. Public reporting does not establish how the vehicle was tasked, whether it autonomously detected or tracked targets, how engagement authority was exercised, or how command-and-control would function in contested conditions. Nonetheless, the test is useful in understanding direction, intent, and progress. As uncrewed systems become more common in the undersea domain, the ability to integrate payloads across different allied platforms will provide the higher degree of operational agility that future operations are likely to require.



Figure 5: A U.S. Mk 48 Heavyweight Torpedo is loaded onto the Royal Navy’s experimental XLUUV XV Excalibur on Sept. 13, 2026. U.S. Navy image

4.2	**If one is good, two is better: A second potential Chinese UUV mothership viewed near Guangzhou** A Chinese vessel resembling a roughly 200-metre ship observed in September in Shanghai, which analysts believe could launch and recover large uncrewed underwater vehicles (UUVs), was observed under tow near Guangzhou. A second UUV mothership hull would suggest China is building a class of UUV support ships rather than a one-off to further enable its growing fleet of extra-large and extra-extra-large UUVs (XLUUV and XXLUUV) to operate both within the First Island Chain and beyond. (source, source, source, source, source, and source) *Assessment:* The vessel was filmed on the Pearl River near Guangzhou in short Weibo clips, which *Janes* found no signs of manipulation in, and bears similarities to the ship observed in mid-September in Shanghai. Built at a different yard and apparently smaller, with six lifting towers to the Shanghai ship's twelve, it points to a family of designs rather than an experiment. Both vessels feature unusual stern structures that could be used to deploy and recover large UUVs, potentially out of sight of commercial satellites, and the Shanghai ship could reportedly carry up to four XXLUUVs. If that assessment is correct, the vessels could support a range of missions including surveillance, seabed mapping, sensor deployment, threatening undersea communication cables and energy infrastructure (a threat earlier DEFTECH Scans have tracked in European waters), and other undersea operations extending into the western Pacific, areas east of Taiwan, and even the Indian Ocean. However, the available evidence remains circumstantial. The Guangzhou ship is unfinished, and imagery alone cannot confirm its role. *Naval News* has noted the absence of key sensors and communications equipment, while *Janes* likewise assesses that the precise purpose of the stern structures remains unclear. Differences in the vessels' size and configuration could indicate related but distinct designs, or they may serve other purposes. The assessment that these ships are likely UUV motherships is consistent with observable trends in China's focus on becoming the global leader in XLUUV and XXLUUV development. Naval analyst H I Sutton asserts that "China's development of extra-large uncrewed underwater vehicles (XLUUVs) is now unmatched globally and accelerating rapidly." China has reportedly developed at least four XLUUVs measuring 15 to 20 metres long and two XXLUUVs measuring 35 to 45 metres, with the XXLUUVs having undergone sea trials in the South China Sea earlier in 2026. The sighting of both ships likely demonstrates that China's efforts to develop systems central to the future of seabed and undersea conflict and competition are being complemented by efforts to develop the logistics and sustainment capability to ensure these systems are available and deployable. The operational value of large UUVs is reduced if they cannot be transported, launched, recovered, maintained, and controlled reliably at sea. Dedicated support ships would help solve those challenges, enabling autonomous systems to operate farther from Chinese territory and remain on station longer.





Figure 6: Two images of the suspected Chinese UUV mothership shared in social media footage from Guangzhou. The lower image shows the amphibious payload bay clearly visible. Six masts possibly serve as a lifting mechanism for a cradle to launch and retrieve underwater vehicles below the hull. Image via Sinodefenceforum, originally Chinese social media.

5. Space

5.1	**Close encounters of the troubling kind: Russian satellite's approach to a commercial satellite tests the resilience of commercial space** In mid-October, the Russian military satellite Cosmos 2612 maneuvered to within roughly 500 metres, according to LeoLabs, of ICEYE-X36, a U.S.-registered commercial synthetic-aperture radar (SAR) satellite operated by Finnish-founded remote sensing company ICEYE. The encounter demonstrates a capability to approach commercial spacecraft widely believed to support Ukraine without mutual coordination and at distances that significantly compress warning and response time. (source, source, source, and source) *Assessment:* According to reporting from *TWZ* and the Center for Strategic and International Studies (CSIS), Cosmos 2612 spent weeks adjusting its orbit before closing on ICEYE-X36, matching its altitude and orbital plane and manoeuvring in close proximity. On 22 October the U.S. State Department called Cosmos 2612's behaviour "threatening", according to *Aviation Week.* The activity demonstrated rendezvous and proximity operations (RPO), a capability with several legitimate applications such as inspection, servicing, and debris management. However, RPO can also have military and national security implications and can serve as another tool in the grey-zone conflict toolkit by holding at risk or damaging satellites—be they commercial or government—supporting military operations during a time of crisis or conflict. As a result, the event demonstrates the growing importance of space-based infrastructure, including commercial satellites, as well as the expanding and destabilizing risks and impacts of counter-space operations. Commercial satellites have become an important component of the intelligence and information architecture supporting Ukraine and military operations around the world more broadly. A constellation operator may be able to replace an individual spacecraft, but an adversary does not need to destroy a satellite to impose costs. Close approaches can create uncertainty, force operators to monitor and potentially manoeuvre assets, consume finite fuel reserves, disrupt collection priorities, and raise questions about what actions could follow. ICEYE emphasized that its constellation is designed for continuity and resilience, and no evidence has emerged that ICEYE-X36 was attacked or impaired. Nevertheless, the episode underscores a growing reality in space operations: resilience is not simply a matter of replacing satellites after they are lost. It increasingly depends on whether operators, governments, and allies can sustain critical services when commercial systems become targets of strategic signalling, pressure, or even attack.

5.2	**Saying the quiet part out loud: U.S. acknowledges on-orbit space-control weapons** U.S. Air Force Secretary Troy Meink publicly acknowledged for the first time on 14 September that the United States has “on-orbit space control weapons capable of defending the joint force against hostile adversary action.” He did not disclose what these weapons are or what they are specifically designed to do. The acknowledgment is a meaningful shift and a deterrent signal, but its deliberate ambiguity may also prompt competitors to invest further in counterspace capabilities. (source, source, source, source, and source) *Assessment:* Speaking at the Air, Space and Cyber Conference in National Harbor outside of Washington, D.C., Secretary Meink confirmed that the United States has "on-orbit space control weapons" but declined to describe their nature, capability, or concepts of employment. Meink did not elaborate on his wording, though the choice to acknowledge the capability while withholding details appears designed to strengthen deterrence. The following day, Space Force Gen. Douglas Schiess similarly stated that Space Force Guardians "operate on-orbit weapons" and would make "disciplined and responsible choices" as the arsenal grows. Space Command separately conducted Apollo Maneuvers, its first live-fly orbital manoeuvre exercise, while reporting shows that several space-based capabilities are under development for the Golden Dome initiative. The public acknowledgment was a notable change in policy. Analysts have long assumed the major space powers were pursuing some form of on-orbit space-control capability. Meink's remarks signal a move toward more explicit deterrence messaging, confirming that the United States fields such systems while withholding the details competitors would most want to know. This ambiguity could strengthen deterrence by forcing competitors to account for unknown U.S. capabilities, but it may also encourage additional counterspace investments as adversaries plan against worst-case assumptions.

5.3	**Congestion, competition, and cooperation: DIA's latest space assessment stresses the blurred line between commercial and military power** The U.S. Defense Intelligence Agency's (DIA) third edition of *Challenges to Security in Space*, released on 26 October, frames space as an increasingly crowded, contested, and interconnected operating environment. The report argues that growing commercial activity, rising military competition, and expanding international partnerships are simultaneously increasing the value of space and its vulnerability during conflict. (source) *Assessment:* The report's central conclusion is stark: "China, Russia, Iran, and North Korea are developing, testing, deploying, and using space capabilities in a way that threatens the security of all space systems and their associated space benefits." It further warns that these countries "have exhibited behaviors that often run counter to a safe, secure, and sustainable space domain." China is, as expected, a primary focus. DIA assesses that Beijing has dramatically expanded its space architecture and now operates more than 510 intelligence, surveillance, and reconnaissance satellites, more than three times its 2018 total. The report also highlights China's military-civil fusion approach, reusable spaceplane program, proximity operations, on-orbit electronic warfare activities, and potential future directed-energy capabilities. At the same time, the report notes growing China-Russia cooperation in space, including technology transfers, component support, and expanding international partnerships through launch and satellite services. The report's most consequential theme, however, is the growing integration of commercial space into national security. DIA notes that the war in Ukraine is demonstrating "the advantages of commercial space capabilities to advance national security activities, including tactical advantages for the military." As commercial imagery, communications, navigation, and data services become embedded in military operations, the distinction between civilian and military infrastructure is increasingly difficult to sustain. Commercial systems are no longer simply supporting conflict; they are becoming part of the operational architecture and, consequently, potential targets. This shift is occurring against a backdrop of unprecedented growth in orbital activity. A recent *SpaceNews* article estimated that there are around 19,000 satellites operating in low-Earth orbit (LEO), reflecting the rapid expansion of commercial constellations and the increasing dependence of governments, militaries, and economies on space-based services. The report argues that congestion, debris, and competition are becoming enduring features of the operating environment rather than temporary challenges. Taken together, the report suggests that space power is becoming less about ownership of individual satellites and more about sustaining services and preserving access. The central challenge is no longer simply placing systems into orbit, but ensuring that communications, intelligence, navigation, and data networks remain available during jamming, cyberattack, orbital interference, and conflict. As commercial and military ecosystems become increasingly intertwined, resilience may prove as important as scale, and access to space services may matter as much as the platforms that provide them.

SCOPE NOTE V

EXECUTIVE SUMMARY VII

DEFINING SPACE 1

DENYING ACCESS TO SPACE 5

CHINA 7

RUSSIA 29

EMERGING SPACE POWERS 43

KEY SPACE DEVELOPMENTS THROUGH 2040 53

OUTLOOK 57

APPENDIX I: SPACE CONCEPTS 59

APPENDIX II: COUNTERSPACE CONCEPTS 67

GLOSSARY OF ACRONYMS 73

SOURCE ENDNOTES 75

Figure 7: The Table of Contents from DIA's Challenges to Security in Space.


deftech.ch