Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

deftech.scan

September 2024

OTH INTELLIGENCE GROUP
Trusted Expertise. Innovative Analysis. Forward Thinking.

https://deftech.ch/scans

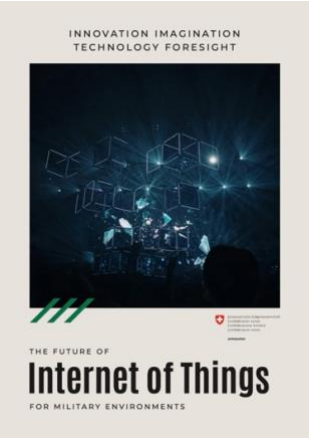
deftech
defencefuturetechnologies

Dear Reader,

With the apparition of the "Unmanned System Force", if some of you had doubts, we can definitely adopt the Apple motto "think different" and try to disrupt our past habits. Legacy systems might not be gone, but will face difficult time.

By a fortuitous coincidence, current events are showing us that some of our considerations on various technologies considered to be 'low tech' or definitely not part of the 'disruptive' ones can still be used to create surprise. This also comfort us in our approach that a technology per se is

This also confirms our approach that the technology itself is rather less disruptive than the way it is used. If not already known, these two documents can therefore be of interest:



https://deftech.ch/iot4sight

https://deftech.ch/low-tech

Before diving into these document, we present you some striking news on the following topics:

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@armasuisse.ch

1. Applications of AI and data

1.1	**Second annual REAIM summit produces "blueprint for action" on military AI** The second annual Responsible AI in the Military Domain (REAIM) conference was held in Seoul, South Korea on 9 – 10 September. Leaders from 60 of the 90 countries that sent representatives agreed to a "blueprint" that attempts to place guard rails around the responsible use of AI. The event offered both hope for broadly accepted standards and practices while still demonstrating the challenges associated with achieving unanimity of opinion on crucial issues related to the military use of AI.. (source) *Assessment:* The first iteration of the Summit was held in February 2023 in the Hague and was designed to build a common understanding of the challenges and opportunities associated with the responsible use of military AI. The Seoul event—co-hosted by South Korea, the Netherlands, the United Kingdom, Singapore, and Kenya—sought to build on the momentum developed in the Hague by moving from understanding to action. The main output of the event was a "blueprint for action" that laid out specific steps and measures that signatory countries agree to take to manage the use of AI in military contexts. Among the details included in the blueprint was language stressing the importance of preventing AI from being used to proliferate weapons of mass destruction (WMD) by actors including terrorist groups and the importance of maintaining human control and involvement in nuclear weapons employment. Leaders from 60 countries signed the plan while 30 countries—including China—sent representatives to the summit but refused to sign the non-binding blueprint for action, reflecting the challenges of gaining global consensus on how AI should be used in military contexts. Netherlands Defence Minister Ruben Brekelmans observed that it was never likely to have all nations agree, but that future summits should address how REAIM signatories "deal with the fact that not everyone is complying . . . that is a complicated dilemma."

Figure 1: The REAIM summit took place in Seoul, South Korea on September 9 - 10. The event involved plenary sessions, an exhibition, and other forums for discussion. The picture above is of the ministerial level attendees representing over 90 countries around the world

1.2	**AI to help reduce civilian deaths** U.S. Special Forces are emphasising the importance of AI in helping to reduce civilian casualties in complex and confusing operational environments in which it can be difficult to discern legitimate military targets from civilian ones.(source) *Assessment:* Christopher Maier, the U.S. assistant defence secretary for special operations and low-intensity conflict, told reporters in late August that U.S. special operations forces (SOF) are investing in AI to help reduce civilian casualties in combat. The U.S. Congress and Department of Defense (DoD) have increased focus on reducing civilian casualties, given the growing number of hybrid threats and potential for U.S. forces to be deployed into environments in which legitimate military targets are comingled with civilians and civilian infrastructure. For example, the FY2023 National Defense Authorization Act ordered the establishment of the Civilian Protection Center of Excellence within DoD. The challenge may be most acute for SOF as they frequently find themselves in urban or complex environments. As a result, Maier says, they will "need the automation and aspects of artificial intelligence and machine learning . . . on the targeting side and the operational side . . . built in and baked into that with a focus on [reducing] civilian harm." Object identification and rapid processing of large amounts of complex data sets can reduce uncertainty about targets, improving the ability of operators to determine what to shoot at and what not to. While this benefit of AI in support of SOF decision-making makes clear notional sense, the use of AI in targeting decisions will only reduce, not eliminate, risk to civilians. Furthermore, the effectiveness of AI and ML in shaping better targeting and tactical decisions comes with two critical caveats. First, AI's ability to increase precision of targeting and reduce civilian casualties will rely on how humans use the information and recommendations AI provides and on the human-developed parameters guiding the AI. Training on and experimentation with AI – enabled tools and intuitive human-machine interfaces are essential to ensuring AI inputs are leveraged in informed and logical manner. Second, increased incorporation of AI into targeting decisions and sense-making on the battlefield places a premium on ensuring the data AI is interpreting is relevant and accurate at the moment it is being acted upon. Absent informed human decision-making and understanding of why AI has made the recommendations and good data, incorporation of AI into targeting decisions may not be effective in reducing civilian casualties in combat.

2. Robotics and Autonomous Systems

2.1	**Unteethered from the routine and expected: Russia adapts to electronic warfare threats with tethered drones** New “Prince Vandal of Novgorod” drones are connected to operators by a fibre optic cable, designed to increase resilience against jamming and spoofing. (source) *Assessment:* Russian forces in Ukraine have used a new type of first person view attack drone that connects to its human controller via fibre optic cable rather than through wireless communication. By physically hard-wiring navigation and communication from the operator to the drone system eliminates the risks of signals being jammed or spoofed and ensures stable communications. As drones have become more prevalent on the battlefield in Ukraine, both Russian and Ukrainian forces have turned to electronic warfare measures such as jamming navigation and communication signals to meet the threat. Use of a system that is essentially impervious from that threat would constitute a tactically useful adaptation on the part of the Russian military. Of course, the use of a physical tether comes with trade-offs. Most notably, the range and manoeuvrability of the Prince Vandal drone is limited by the length of the wire available, meaning that this type of drone might be relevant in certain types of close in missions. While Russian sources originally claimed the capability was indigenously developed, additional unverified reporting from independent observers and bloggers focused on the conflict in Ukraine has emerged that claim the drones are actually imported Chinese Skywalker commercial drones known for their fibre optic cables.

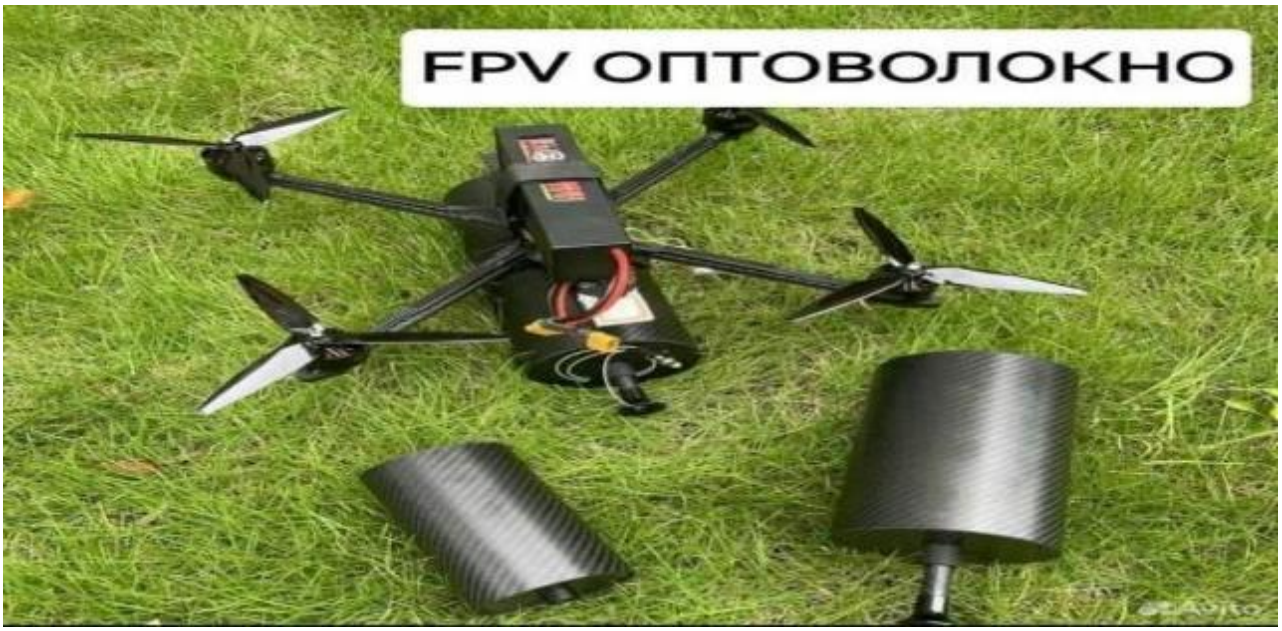


Figure 2: A photo of the Vandal Prince of Novgorod drone that uses a fibre optic cable to ensure secure communications. Source: Facebook

2.2	**House of the Dragon: The dragon war comes to Ukraine** Ukraine has deployed drones capable of launching molten metal at Russian forces. Videos of the drones in action have been posted to social media associated with the Ukrainian armed forces. (source) *Assessment:* In late August, CNN reported that Ukrainian forces had deployed "dragon drones" that spray the molten metal thermite at targets on the ground. Thermite is a mixture of aluminium powder and iron oxide that burns at 2,200C / 4,400F and burns through most substances, including metal. When launched from a drone it resembles a dragon spewing fire. Videos posted on social media and by Ukraine's Ministry of Defence demonstrate the devastating physical and, especially, psychological damage that thermite attacks—and incendiary weapons more broadly—can produce. The drones have been employed to drop thermite on treelines to burn away canopies, burn away canopies and kill or destroy enemy personnel and assets within the affected area. Thermite is not new to warfare, having been used in both World War I and II and there have been reports that Ukraine has previously used thermite to disable Russian tanks earlier in the war. In addition, roughly a week after the CNN reporting on Ukraine's use of thermite spewing drones, a video of Russian thermite drones also surfaced. The Russian video show less damage but reinforce the adaptive and frequently escalatory dynamic that has marked the drone war in Ukraine.

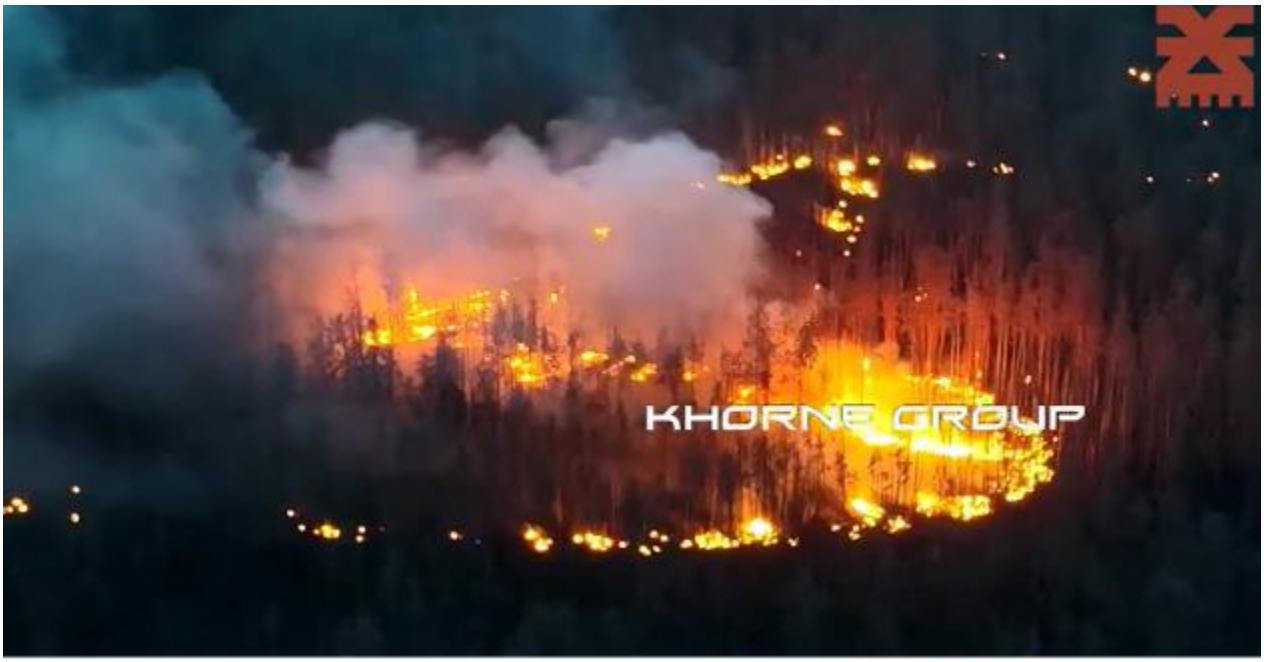


Figure 3: A screenshot from a video posted on social media reportedly showing the impact of a "dragon drone" attack outside of Kharkiv. Source: Khorne Group via Telegram, CNN

2.3	**North Korea unveils new loitering munitions** State media KCNA released photos of Kim Jong Un visiting the Drone Institute of the Academy of Defence Sciences on August 24. The new loitering munitions strongly resemble Israeli systems and have also drawn comparison to Russian and Iranian systems. (source, source—subscription required) *Assessment*: The photographs show two unnamed loitering uncrewed aircraft systems (UAS), which analysts have described as being virtual copies of the Israeli-made delta wing Harop and cross-wing designed Hero-400 loitering munitions. In addition, some comparisons of the cross-wing system have been made to the Iranian Omid and Russian Lancet. Despite the photos being heavily pixelated, *Aviation Week* assessed that the electro-optic payload for each aircraft "appears to be rudimentary when compared to their Russian [Lancet] and Israeli [Harop] counterparts." No technical specifications were released with the photos, though state newspaper *Rodong Sinmun* reported that "the drones to be used within different striking ranges are to perform a mission to attack any enemy targets on the ground and in the sea. The drones of various types correctly identified and destroyed the designated targets after flying along different preset routes." North Korea's development of loitering munitions makes sense for a country seeking lower-costs options for increasing its capacity to attack enemy forces both along the front lines or deeper behind a conflict zone. Harop drones were originally designed for anti-radar mission, though they have been deployed against artillery pieces and other forces. State media reported that the cross-wing system successfully destroyed a mock South Korean main battle tank.

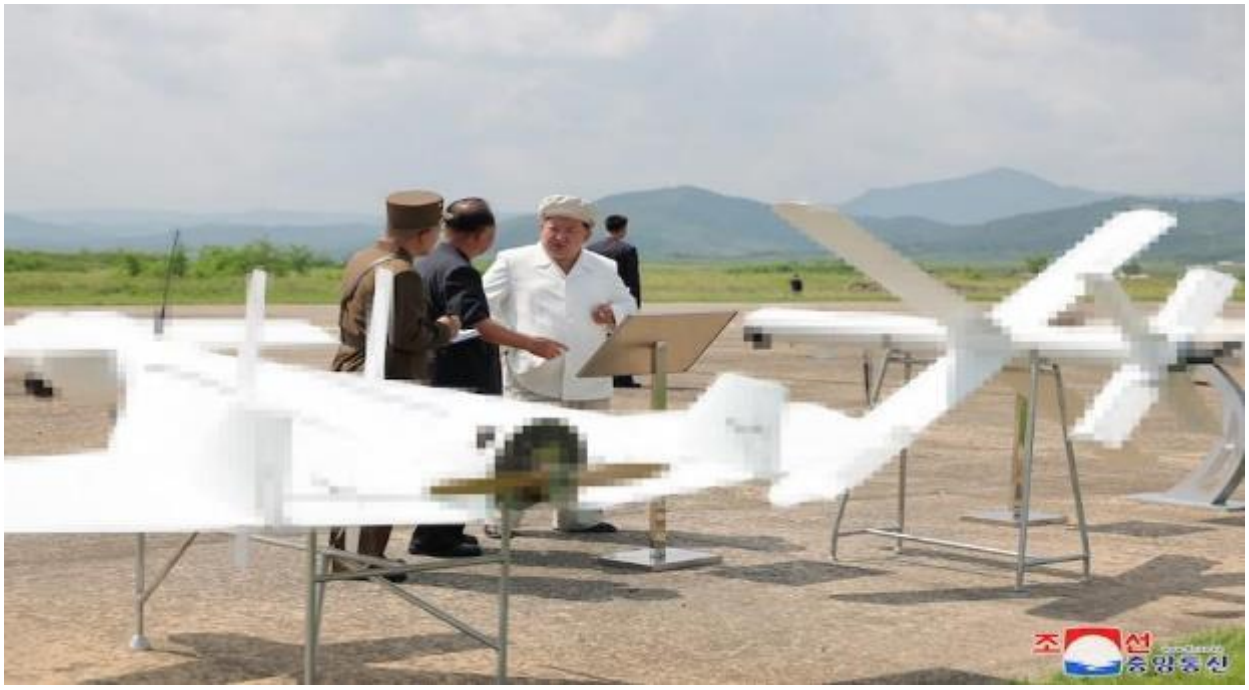


Figure 4: North Korean state media organization KCNA released the above photograph of Kim Jung Un inspecting two loitering munitions. Source: KCNA, Aviation Week

2.4	**U.S. Army tests autonomous equipment decontamination system** The uncrewed ground vehicle (UGV) accelerates the process of assessing biological and radiological contamination levels of military equipment. (source) *Assessment*: The value of uncrewed systems is frequently framed as being able to carry out the dull, dirty, and dangerous tasks more efficiently and safely than human operators. On 12 August, the U.S. Army announced that earlier in the year, four solders from the 1st Armoured Division tested an autonomous ground vehicle designed to carry out one of those dull, dirty, and dangerous missions: decontamination of military equipment exposed to chemical and biological toxins. Known as the Autonomous Equipment Decontamination System, the vehicle consists of a camera mounted on a UGV. The camera scans the entire vehicle surface as it circles around it, transmitting the contamination data back to the system operators seated at a computer at a safe distance away from the inspected vehicle (s). A robotic manipulator arm then uses that data to spray a decontamination slurry developed by the Army targeted on exposed areas, conserving decontaminant and saving time, according to Army reporting on the test. Currently, it takes a team of 20 to 30 soldiers in full protective gear 45 to 60 minutes to contaminate each vehicle exposed to chemical or biological hazards. Moreover, these soldiers must perform this task close to the point of exposure putting them in a higher degree of risk of contamination and of vulnerability to enemy fire. The process takes more than 500 gallons of water and 50 gallons of decontaminant per vehicle. One of the key elements of the test, which was held as part of the Manoeuvre Support and Protection Integration eXperiments event in May, was that the operating crew was able to meet face-to-face with system designers to provide direct feedback. This interaction is a crucial element of technology development and adoption that is frequently excluded or minimized in the innovation process. Sergeant First Class Joseph Bennett told Army media that “We usually never get a chance to meet the people designing the instruments we’re using as soldiers. So, getting to experience the brain behind the equipment was exciting. They’re coming to us and asking, ‘Is this what you really want?’, and we get to tell them what to think.

Figure 5: The Autonomous Equipment Decontamination System being tested in May. Source: U.S. Army

2.5	**Suspicious drone activity near military bases and critical infrastructure in Europe** Multiple suspicious drone-related incidents took place proximate to critical infrastructure and military bases in Europe during the reporting period. Questions persist about the intent and identify of those responsible. These types of risks have grown more common in an age of rapid and broad diffusion of commercial drones that can easily be applied for "dual use" surveillance or strike missions. (source and source) *Assessment:* A series of suspicious drone-related incidents took place in Germany in August. One incident involved several nocturnal drone flights spotted over a geographical area that included several critical infrastructure nodes, including a defunct nuclear power plant, a large chemical factory, and a liquid natural gas terminal. The uncrewed systems reportedly exited the area at speeds over 100 km an hour after being spotted, outrunning police drones. Earlier in the month, Geilenkirchen NATO airbase was temporarily put on the second highest alert after foreign intelligence suggested a threat might be imminent. The nature of the threat has not been revealed, though reports indicate that at least part of the threat may have been drone-based. A NATO spokesperson later told reporters that no drones flew over the base, though there was no additional information about whether drones had been sighted near the base. Unidentified drones have also been reported over other German military bases, including those at which Ukrainian military personnel are trained, raising concerns that suspicious incidents may be linked to Russia. No government officials have formally confirmed that link. Overall, German newspaper "Süddeutsche Zeitung" reported in August (and an additional link for an English-language reference) that there have been over 400 unidentified drone flights over or near restricted German military bases since 2023. Similarly, on the evening of September 8 and early morning of September 9, Stockholm's Arlanda airport, the largest airport in Sweden, was shut down for 2.5 hours after four unidentified drones were detected over the airport. Authorities have not identified the types of drones nor have they commented on who was responsible for the incursion.

3. Digital Communications and Cyber

3.1	**Western intelligence agencies highlight persistent Russian cyber activity** Germany, Poland, the United States and others all raised awareness of the Russian hacking threat against Europe and NATO allies and also took targeted action against purported Russian hacking groups. (source, source, and source)

Assessment: Several developments related to Russian hacking efforts took place during the reporting period.

On 9 September, Poland's security services announced they had broken up an alleged cyber sabotage group linked to Russia and Belarus that attempted to "paralyze" the country with cyberattacks. Poland's Minister of Digital Affairs, Krzysztof Gawkowski, referred to the group's activities as a "de facto cyberwar." Gawkowski also observed that cyberattacks on Poland have doubled since last year, amounting to more than 400,000 incidents in the first half of the year.

Also on September 9, the German domestic intelligence agency released a declaration that accused Russia's Unit 29155 of carrying out cyber-attacks against Western countries supporting Ukraine since the start of Russia's invasion of Ukraine in February 2022. The declaration was also signed by intelligence agencies in the Netherlands, Czech Republic, Estonia, Latvia, Canada, and Australia. Specifically, the declaration said that the group—also known as Cadet Blizzard and Ember Bear—was responsible for the WhisperGate campaign, a coordinated attack on Ukrainian government agencies in January 2022. It also claimed Unit 29155 has focused on attempts to "scout and disrupt" aid deliveries to Kyiv in the more recent past.

Keir Giles, an expert on Russian cyber activities at the UK-based Chatham House think tank told the *BBC* the announcements made it clear "that the targets were much broader than (just Ukraine), and they're talking about a range of different government and civilian agencies, civil society agencies across Western Europe and across the EU and NATO" that have been targets of cyber-attacks.

In a related development, on 5 September, the U.S. Department of Justice charged five members of Unit 29155 and one civilian with conspiracy to commit computer intrusion and wire fraud conspiracy associated with the WhisperGate campaign. According to the Department of Justice, "The GRU's WhisperGate campaign, including targeting Ukrainian critical infrastructure and government systems of no military value, is emblematic of Russia's abhorrent disregard for innocent civilians as it wages its unjust invasion." All of the indicted individuals live in Russia.

3.2	**The silent threat: UK to build advanced facility to test against electronic warfare threats** The facility will be among the largest and most advanced in Europe. The announcement, along with announcement of a new electronic warfare centre of excellence in Australia, reinforce the growing importance of electronic warfare and the perceived vulnerability of many cutting edge platforms to these threats. (source) *Assessment:* On 21 August, the UK Ministry of Defence (MoD) awarded a £20 million contract to QinetQ to build a "silent hangar" radio frequency, anti-jamming test facility. The test facility will be large enough to fit many of the UK's largest aviation assets such as the F-35, Chinook helicopters, and Protector drones. The increasing prevalence of "hostile threats jamming GPS to disorientate military equipment" is driving a need for heightened resilience to a more diverse set of electronic warfare threats, according to MoD representatives. The hangar will reduce reflections, echoes or the escape of radio-frequency waves. The facility's GPS simulators and threat emulators inside the hangar will allow the UK to test its aircraft against several simulated hostile environments and distinct offensive electronic warfare threats. The facility is set to open in 2026. Also during the reporting period, L3 Harris inaugurated a new electronic warfare centre of excellence in Brisbane, Australia. The facility will incorporate the design, production, integration, and maintenance services of electronic warfare solutions used in advanced tactical missions. It will also be used to increase domestic manufacturing capabilities and opportunities in areas such as robotics, data management, quantum sensing, and communications.

3.3	**"Spooky action at a distance": Boeing to test quantum entanglement swapping** The experiment could serve as a building block for a quantum communications network that could link quantum computers and sensors and enable new types of enhanced sensing and communications capabilities. (source and source) *Assessment:* Reporting from 10 September shows that Boeing plans to launch its Q4S satellite in 2026 to demonstrate quantum entanglement swapping, described by *Aviation Week* as "a process in which two pairs of quanta—in this case, photons—become linked so that a change to one immediately affects the other no matter their distance apart." Alber Einstein referred to the phenomenon, which allows for quantum teleportation of information, as "spooky action at a distance." The system will use a process called spontaneous parametric down-conversion to entangle the photons. Through this process, a laser beam is passed through a nonlinear optical crystal to split one photon into a pair of entangled photons. After creating two pairs of photons, a photon from one pair is then entangled with a photon form another, thus swapping entanglement between the two sets. If the two sets of photons in a future quantum communications network were paired at distant locations and one of each pair was sent via laser to a satellite, the entanglement of those photons at the satellite would also instantaneously entangle those left on Earth. Boeing believes that this capability is critical to the development of quantum sensing and communication capabilities as well as the development of extremely precise time synchronization, which could be used to improve position, navigation, and timing of platforms and systems.

3.4	**France achieves world's first space-based laser communications test** The test took place earlier in the summer and involved using lasers to communicate between a low-orbit nanosatellite to a commercial ground station. The French MoD labelled the achievement a world's first in optical high-speed communication. (source) *Assessment:* Two French companies, in coordination with the French Defence Innovation Agency, established a stable optical link between a nanosatellite in Low Earth Orbit (LEO) and a ground station for several minutes. The tests opens the way for the use of the system on future French military satellites as well as other military assets. According to the French MoD, the success makes it possible to use space-based laser communications on "mobile, land-based, naval, and airborne platforms." The optical link offers advantages over traditional radio frequency communications in space, including accelerated speed of communication, enhanced security, and independence from constraints associated with radio spectrum coordination regulations. The focus on speed and security is vital in a context in which timely and accurate information is necessary to making informed decisions and to the identification of targets such as hypersonic missiles in an increasingly time compressed environment. The Defence Innovation Agency provided €5.5 million in funding to the two French companies involved in the programme. Cailabs' technology and photonics expertise enabled development of a reliable and robust ground station capable of receiving laser communications from space. Unseeable's nanosatellites enabled the integration of the laser payload within the short timeframes demanded by what the MoD referred to as the "New Space Pace."

4. Human Performance and Protection

4.1	**The limits of technology: Skill, leadership, and experience still matter in combat** In a recent U.S. Army exercise, "old school" soldiers defeated a larger force armed with more advanced technology in a tactical wargame that reveals the limits of novel technologies and the importance of tactical expertise and experience and leadership in combat. (source) *Assessment:* On 27 August, *Defense One* published a description of a recent exercise involving elements of the 101st Airborne division and a reconnaissance force known as Geronimo. The Geronimo team serves as the Red Team in realistic wargames to prepare units for deployment. The exercise involved a 101st Airborne unit known as Strike facing off against a Geronimo unit called Ghost. The Strike team, which outnumbered Ghost three to one, was equipped with brand-new drones, electronic warfare tools, loitering munitions, night vision goggles, and very quiet Infantry Squad Vehicles. The Ghost team rode on small, but loud, all-terrain vehicles and was equipped only with a TSM-800 drone. The TSM-800 flies along a fixed route that follows preset waypoints and is unable to redirect to promising targets. The Ghost team held at least two advantages. First, the team consisted of experienced soldiers who have been involved in similar exercises several times a year and are very familiar with the terrain in which the exercise took place. Second, the team was able to recover in air-conditioned rooms between missions rather than being stuck in the extreme heat of the training environment. The article provides a blow-by-blow description of the Ghost team's efforts to find the 101st's Multi-Function Reconnaissance Company (MFRC), one of only three units across the Army equipped with modern technology described as "perfect for hunting the adversary." The narrative largely focuses on how the Ghost team was able to use its tactical nous and experience to avoid detection and locate enemy forces dispersed throughout the training area. The piece serves as a useful reminder that even in an age of increasingly rapid development and diffusion of novel technologies, leadership, experience, and superior knowledge of terrain can in many cases counteract the advantages of these technologies. Moreover, the episode also demonstrates the importance of creating challenging wargame environments and rules that force units to cope with and learn from adversary and even defeat.

4.2	**Adjacent innovations and the need to organize for the uncrewed fight** The Ukrainian parliament has adopted a bill that establishes the Unmanned Systems Force (USF) as a new branch of Ukraine's military services. The formal adoption of the unit comes after months of discussion and preparation within Ukraine's armed forces. (source and source) *Assessment:* The bill passed in early September is the culmination of a process that began in February when President Volodomyr Zelenskyy directed Ukraine's Cabinet of Ministers and General Staff to develop proposals for the creation of the USF. In June, Colonel Vadym Sukharevskyi was appointed as the commander of the nascent unit, a move that was followed shortly thereafter by the government sending a draft law to the Ukrainian parliament for discussion and approval. Analysis in June of the prospect of the standing up of Ukraine's USF from *Long War Journal* notes that The Ukrainian military includes three branches: Ground Forces, Air Force, and Navy. It also includes independent combat arms, such as Special Operations Forces and Support Forces. The bill places the USF in the second category of independent services. According to comments from Colonel Sukharevskyi in June, the USF has over 3,000 personnel and is actively recruiting. The main mission of the USF will be to "systematize and scale up" Ukraine's use of uncrewed systems, ensuring that the successes that have been documented in media are "replicated across the entire front." This will require establishing "a unified tactical doctrine to maximize results across all units", ensuring uncrewed systems units are well equipped and supplied, and devising means of scaling the bottom-up tactical and operational innovations that are happening at unit levels but are not necessarily being shared across the force. The formal establishment of the USF reflects the challenges of scaling adoption of emerging technologies and the need for non-technical innovations in adjacent areas such as organizational development, training, recruitment, doctrine, and procurement. Ukraine views uncrewed systems as a force multiplier and a means of competing against a larger Russian military with access to more materiel. Building a new organization charged with scaling uncrewed systems development and use, then, is a crucial next step to exploiting the advantages uncrewed systems provide in a durable and resilient way. As Ukraine's first deputy minister of defence, Ivan Havrylyuk, declared in February "the Unmanned Systems Forces can be our asymmetric answer to the aggressor's quantitative superiority."

5. Platforms and Weapons Systems

5.1	**China's new standoff electronic warfare plane breaks cover in Thailand** The Y-9LG electronic attack platform participated in a late August exercise with the Royal Thai Air Force. The system possesses an innovative design and is the most recent addition to China's expanding special missions fleet. (source) *Assessment:* The Y-9LG aircraft is understood to be a long-range jamming platform. While it was first spotted in 2017, it did not enter service in the People's Liberation Army Air Force (PLAAF) until 2023 and has been rarely seen in open sources since. The aircraft's innovative design features a 'balance beam' radar antenna mounted above the fuselage. This balance beam is understood to contain an array used for offensive electronic warfare including emitting electronically scanned radar beams to jam enemy radar signals from a stand-off distance. In addition, the aircraft's enlarged nosecone is presumed to carry another electronic warfare antenna. Fairings on the sides of the rear fuselage likely serve side-looking electronic intelligence or electronic support measures (ESM) antennas. Additional ESM antennas are installed below the forward and rear fuselage and atop the tailfin. The presence of ESM antenna's means the Y-9LG can serve in an intelligence, surveillance, and reconnaissance system. The Y-9LG is designed to operate from a standoff position, leveraging its powerful radar to electronic attack against adversary communications systems or detect signals and collect data in the electromagnetic spectrum that could help either kinetic or non-kinetic targeting. *The War Zone* points out, though, that there are concerns about the survivability of platforms like the Y-9LG in a high-intensity conflict against a peer adversary. The sensors require a line of sight to the targeted emitter to perform their functions, potentially placing them in a detectable range.

Figure 6: The Y-9LG electronic warfare aircraft in action during Exercise Falcon Strike in Thailand in late August. Source: X account of Rupprecht_A, 30 August 2024

5.2	**Hard to kill: People's Liberation Army (PLA) exercise demonstrates the challenge of defending against drone swarms** Test revealed the need for layered approaches to drone swarm defence that incorporate both kinetic and non-kinetic weapons. (source) *Assessment:* The PLA acknowledged that it achieved only a 40% hit rate in using anti-aircraft artillery against an attacking drone swarm during a recent exercise. State broadcaster CCTV quoted one exercise participant as saying "shooting at drone swarms was still quite challenging due to their speed and small size, as well as their ability to change flight trajectories—making it easy for gunners to lose their targets." The low strike rate reflects the complexity of the drone swarm defence challenge. Any single defensive solution is unlikely to be able to defeat 100% of the threat. As a result, concepts of drone swarm defence increasingly focus on the need for a layered and multi-faceted approach to drone swarm defence that incorporates multiple types of non-kinetic solutions such as lasers and high-powered microwaves as well as jamming and spoofing. These solutions could complement kinetic solutions such as anti-aircraft artillery and close-in weapons systems and build resilience of drone swarm defence systems.

https://deftech.ch/