Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

DEFTECH-SCAN

November 2025

OTH INTELLIGENCE GROUP

deftech.ch/scans

Dear Reader,

This month's DEFTECH Scan navigates a landscape where systems are increasingly "commanded, not controlled" — a subtle but telling shift from the usual "human in, on, or out of the loop."

From AI copilots whispering in the ears of fighter pilots to drones that think faster than their operators, from encrypted dreams to unguarded satellites, this edition tracks technology's stubborn refusal to stay in its box.

If foresight had a sense of humor, it might say: ***the future is not out of control — it is just following different orders***. *(Smile)*

As the horizon continues to shift, several developments merit attention::

1. **Applications of AI and data** **2**
2. **Robotics and Autonomous Systems** **4**
3. **Connectivity** **7**
4. **Human Protection and Performance** **10**
5. **Platforms and Weapons Systems** **13**

Proceed with curiosity; the future rarely behaves as briefed.

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	**Ol' Blue Eyes: Danish company developing AI for real-time ordnance detection** Dropla has developed its Blue Eyes system specifically to provide real-time explosive detection in contested environments where connectivity is compromised. The system should help reduce risks to front-line Ukrainian troops from Russia's ambush drones (source and source) *Assessment:* The deployment of new technologies and capabilities, and shifting operational realities, has led to an increase in risks for resupply convoys along Ukraine's "zero-line." One example is Russia's use in recent months of explosive-laden "ambush drones" and landmines that are fired from Russia's side of the front-line to lie in wait to ambush resupply vehicles. According to reporting from *Business Insider*, "when a convoy approaches, these ambush drones can blindside their targets from as little as 30 feet away." Federico Borsari, a researcher on drone warfare at the Center for European Policy Analysis (CEPA), assessed that these ambush drone tactics can have a significant effect on the battlefield and "completely disrupt the entire logistical chain." Denmark-based Dropla has developed its Blue Eyes software to help manage this new challenge. The software processes video feeds from cheap quadcopters as they fly over supply routes in real-time. The operational concept for Blue Eyes' use involves surveillance drones scouting the routes just ahead of a convoy. Blue Eyes analyses the thermal and optical footage collected by the drones, quickly highlighting anti-tank and anti-personnel mines. Once an enemy landmine or drone is detected, Blue Eyes sends its coordinates to Ukraine's battle management system, providing commanders with vital decision-making intelligence. Blue Eyes' value is in greatly enhancing situational awareness and accelerating the processing of intelligence. The company has over two dozen engineers in Ukraine working to train the company's AI model to detect more than 170 different types of explosive threats, including landmines and idling quadcopters, on local battlefield terrain. In addition, Dropla also claims that Blue Eyes' "autonomous architecture enables reliable deployment in denied or degraded network environments, including contested electromagnetic spectrum conditions with active electronic warfare interference.

1.2	**AI battle management system incorporated in a fighter jet test** U.S. fighter pilots have, for the first time, received real-time battle directions from an AI system during a Pentagon-led joint exercise—a significant step for the integration of artificial intelligence directly into combat operations (source and source) *Assessment:* The test featured an aerial battle management system known as Starsage that guided human pilots flying F-16, F/A-18, and F-35 jets with tactical instructions normally provided by human controllers on the ground. The Raft AI technology reportedly reduced response time from minutes to seconds, providing instant threat alerts and mission updates straight to the pilots. The applications for this technology for pilots are broad. Certainly, the ability to receive intelligence on hostile actors, their capabilities, and likely intent and actions nearly instantaneously offers an advantage in operational and tactical environments that are marked by complexity and speed. However, Starsage can also help manage air traffic in these environments, including blue force tracking so that pilots are able to avoid one another. For example, Raft AI CEO Shubhi Mishra claimed that these types of systems could have helped prevent the midair collision that occurred between a commercial regional airline and a Black Hawk helicopter near Ronald Reagan National Airport outside of Washington, DC earlier in 2025 in which 67 individuals died.

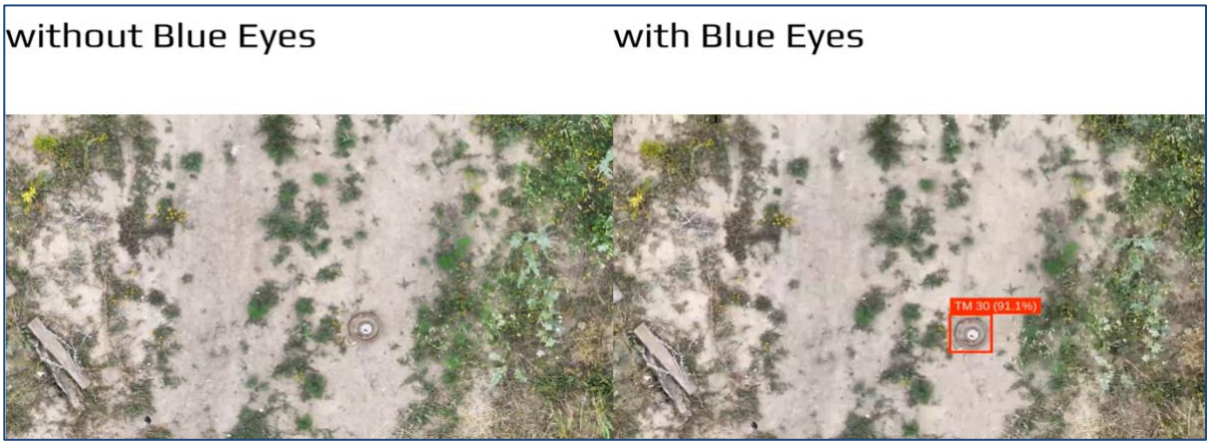

Figure 1: Side-by-side images from Dropla's Blue Eyes product page showing the value the system brings in flagging landmines and ambush drones. Source: Blue Eyes product page

2. Robotics and Autonomous Systems

2.1	**More progress and testing for Australia's MQ-28 Ghost Bat** Boeing Australia and the Royal Australian Air Force (RAAF) are planning two significant tests for the MQ-28 Ghost Bat collaborative combat aircraft (CCA) to further validate the aircraft's concept of operation and viability. Additionally, Boeing has released images that suggest it is capable of a broader range of missions. (source and source) *Assessment:* The Ghost Bat is already among the most mature of the CCA programs currently under development globally, and upcoming tests are designed to demonstrate progress made in the program since its inception in 2017. Boeing Australia announced in October that the uncrewed aerial system (UAS) will have a flying demonstration in 2026. The test flight will include the Ghost Bat being controlled by a pilot in a fighter jet as part of ongoing efforts to prove the viability of the concept of CCAs working with crewed aircraft. In the summer of 2025, a Royal Australian Air Force (RAAF) E-7A Wedgetail successfully controlled an MQ-28 during a simulated mission. The Boeing official did not identify which fighter jet would be used for the test, though options include the Boeing F/A-18E/F Super Hornet, the Boeing EA-18 Growler electronic warfare aircraft, and the Lockheed Martin F-35. The inclusion of a Lockheed Martin aircraft as a possibility reflects the program's emphasis on modularity and open-architecture systems and ability to integrate with non-Boeing-produced aircraft. Boeing has also announced that the Ghost Bat is expected to launch a Raytheon AIM-120 AMRAAM missile at a flying target from an MQ-28 Block 1 by the end of the year. Additionally, according to *The War Zone*, recent computer-generated video from Boeing includes MQ-28s with apparent receptacles on top of the drone's fuselages to enable aerial refuelling from boom-equipped tankers. The capability to refuel mid-air would extend the MQ-28's range and on-station time—and as a result its mission flexibility—though likely with the trade-off of increased cost and design complexity. The announcement was made during the Asian Defence Exhibition held in October in Korea, reflecting Boeing Australia's ambitions to export the MQ-28 beyond the RAAF. While these tests represent significant steps forward for the program, the UAS is not expected to enter service until at least 2027.

Figure 2: A screen capture from the Boeing Video that apparently shows an aerial refuelling capability for the MQ-28. According to analysis from The War Zone, the hatch at the front of the fuselage (painted white with black striping) is similar in design to the aerial refuelling hatch on F-35s. Source: The War Zone

2.2	**Ukraine unveils a new extra-large uncrewed underwater vehicle (UUV)** The TLK-1000 marks a significant increase in size and capability for the Toloka series of maritime weapons and could provide a new threat to Russian military and critical infrastructure (source and source) *Assessment:* Ukraine has used uncrewed maritime vehicles during its conflict with Russia, though the relatively small size of the warheads of systems such as the TLK-150 has reduced the ability of these systems to do lasting damage to large infrastructure. The TLK is the first system in the Toloka family, developed in April 2023. While it is shaped like a UUV, the system actually operates just below the surface of the sea and relies on sensors and communications capabilities on a mast that operates above the surface. It has been described as "effectively a smart, electrically powered torpedo which can loiter for days at a time waiting for a target." In 2024, Toloka began developing two larger systems. The TLK-400 is around 40 feet long and has a hybrid propulsion system, giving it a range of around 800 miles and an endurance of two months. It can operate at depths of up to 1,000 feet. Typical missions include reconnaissance, minelaying, communications relay, and direct attack. It can carry a 1,000-pound warfare, making it more powerful than the U.S. Mk48 heavyweight torpedo. The TK-1000 was shown at an exhibition in Lviv for the first time in September. It is an extra-large system of up to 12 metres with a payload of five tons. Typical missions are given as "destruction of large stationary targets", such as bridges and bases. It can also lay mines. It appears that its range and endurance are similar to those of the TLK-400. Toloka claims the UUVs are autonomous, with neural-network-based AI for sensing and navigation, though this level of sophistication may not be necessary for undersea systems, depending on the mission—for example, if their task is only to navigate to a spot to lay a mine or detonate a bomb. Nonetheless, the focus on these much larger systems reflects the utility of autonomous uncrewed systems across domains, particularly in the undersea domain, where detection and communication of threats is especially difficult.

Figure 3: The relative dimensions of the Toloka series of uncrewed maritime vehicles. Source: Toloka

2.3	**UK Defence Innovation announces initiative to develop a collaborative UAS for rotary wing aircraft** The organisation released a tender on 4 November describing the program and tender process for the development of a Capability Concept Demonstrator (CCD) for the Land Autonomous Collaborative Platform (ACP) project, known as Project NYX (source) *Assessment:* The Project NYX program seeks to pair an autonomous UAS with the Apache AH-64 attack helicopter to operate in a highly autonomous "commanded not controlled" manner. The UAS will improve the lethality and survivability of the crewed helicopter with lower logistics and maintenance burdens than crewed aircraft. Specifically, the tender documentation lists several multi-mission tasks that the UAS will carry out, including reconnaissance, target acquisition, strike, countermeasure defeat, and integration with Launched Effects (LE). Priority technical areas of interest for the program are: • Integration and interoperability considerations with existing Ministry of Defence (MoD) communications networks and hardware • Specification, development, assurance, and management of autonomous behaviors • Situational awareness systems for ACPs within human-machine teaming • Modular Open Systems Architectures for ACPs • Defence Lines of Development considerations, including safety, interoperability, and cyber security A contract award for up to four suppliers for initial development is expected to be made in Q1 of 2026 with the end of the CCD program set for Q1 of 2028. The total estimated value of the awards is £100,000,000. The concept of collaborative autonomous UAS operating in conjunction with crewed aircraft has gained real momentum over the last five years, as highlighted in the above discussion of the Ghost Bat CCA. However, most of this momentum has been focused on capabilities that pair with larger fixed-wing aircraft, such as fighter jets and surveillance aircraft that fly at higher speeds and higher altitudes. The use of collaborative UAS in support of helicopters seems an inevitable extension of this concept that can help improve the lethality and survivability of helicopters in increasingly crowded and contested airspace. Still, it comes with unique challenges related to the distinct environment in which helicopters tend to operate. Helicopters fly at lower altitudes and speeds, frequently in low light conditions, and are more vulnerable to difficult-to-detect and target short-range weapons that reduce survivability and place a premium on speed of communication and situational awareness. This challenging and very fast-moving environment complicates the use of ACPs while also driving demand for these systems.

3. Connectivity

3.1	**Under a (very) bad sign: Researchers uncover concerning vulnerabilities in civil, commercial, and military satellite communications** Researchers at the University of California-San Diego (UCSD) and the University of Maryland passively collected a stunning variety and volume of data that has been transmitted from Geostationary Orbit (GEO) to Earth unencrypted, including sensitive military data and personal phone call and text information (source) *Assessment:* The researchers spent three years developing and using an off-the-shelf, $800 satellite receiver system to capture the communications of GEO satellites in the small band of space visible from the roof of a building at UCSD in Southern California. The team pointed their dish at different satellites in GEO and then spent months interpreting the signals they received. The captured communications included samples of the contents of personal calls and text messages on T-Mobile's network as well as other networks in Mexico, data from airline passengers' in-flight Wi-Fi browsing, communications to and from critical infrastructure such as electric utilities and offshore oil and gas platforms, and U.S. and Mexican military and law enforcement and military communications that revealed the location of personnel, equipment, and facilities. The researchers have reached out to all of the organizations that were found to be communicating unencrypted sensitive information to make them aware of the vulnerabilities. Aaron Schulman, a professor at UCSD who led the process, told *Wired* that the findings of the research "completely shocked" the team, adding that "there are some really critical pieces of our infrastructure relying on this satellite ecosystem, and our suspicion was that it would all be encrypted." One of the other study participants noted that the team did not actively intercept any communications, but rather passively listened in on what was being "broadcast to over 40 percent of the Earth at any point in time." Essentially, anyone capable of assembling a similar low-cost receiver system could also capture these signals. Among the most sensitive information were unencrypted internet communications from U.S. military maritime vessels and sensitive information about counter-narcotics operations from the Mexican security forces. The researchers also collected military asset tracking and maintenance records for military aircraft like Mil Mi-17 and UH-60 Black Hawk helicopters, naval vessels, and armoured vehicles. Sensitive information from the Mexican and U.S. critical infrastructure, including unencrypted satellite communications for industrial control system software, was also collected. The researchers raised concerns with critical infrastructure operators that malicious actors might be able to potentially disable or spoof these systems, affecting their operation. While some of the affected companies and organizations have taken proactive steps to encrypt their satellite communications, not all have. This is concerning, given the low cost of developing a system capable of replicating this experiment. One analyst interviewed by *Wired* captured the nature of the enduring challenge: "This was not NSA-level resources. This was DirecTV user-level resources. The barrier for entry for this sort of attack is extremely low." This is especially the case because the researchers are releasing their own open-source software tool for interpreting satellite data on GitHub.

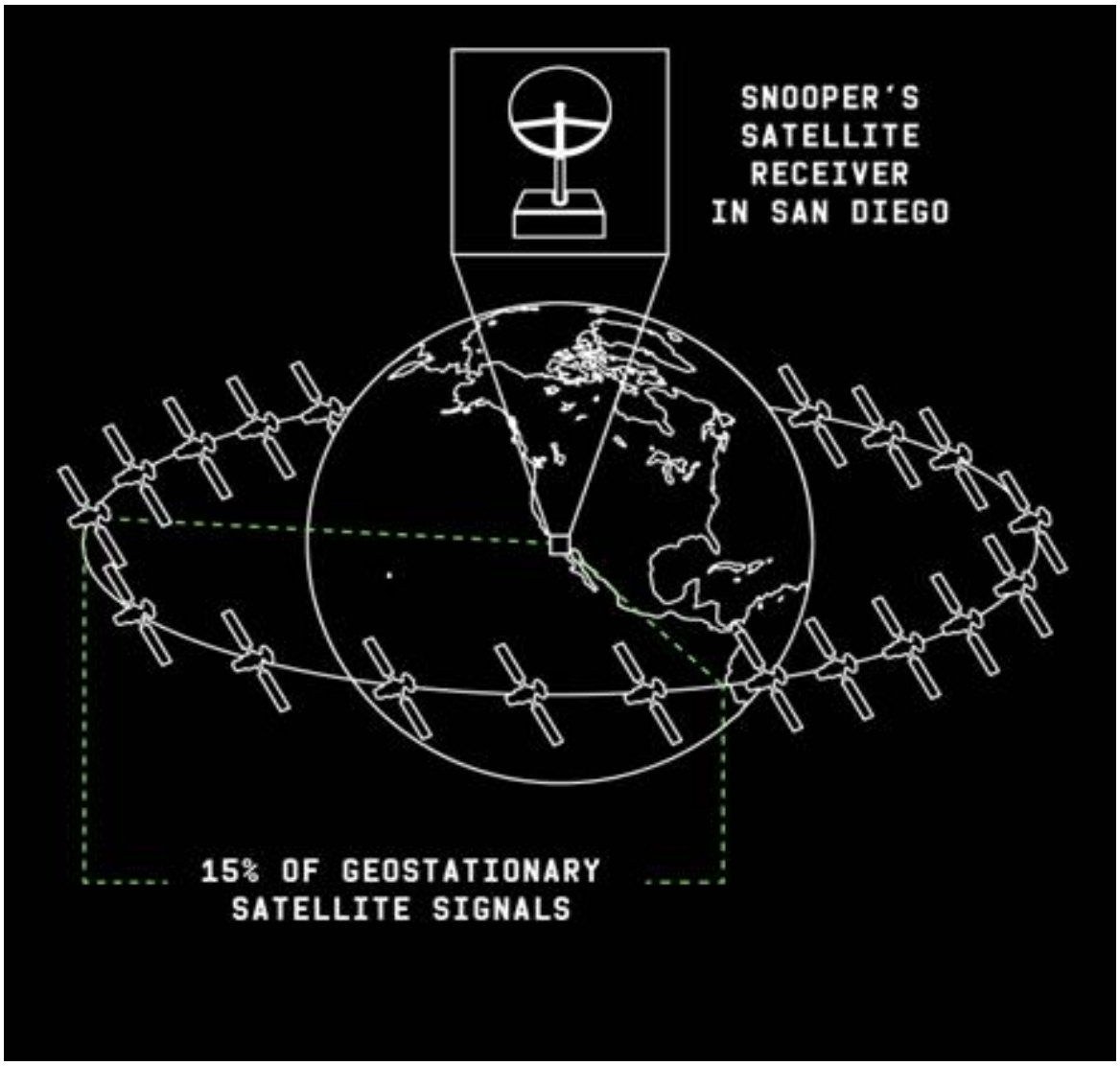

Figure 4:A depiction of the small piece of GEO orbits from which the research team's receiver could detect signals. Source Wired

1.3	**Man bites dog and other stories from the cyber frontier** China accused the United States of hacking into sensitive government systems during a busy reporting period for cyber conflict (source, source) *Assessment:* On 18 October, China's State Security Ministry released a statement on the organization's WeChat account accusing the United States' National Security Agency (NSA) of carrying out a cyberattack operation against China's National Time Service Center dating back to at least 2022. The breaches were used to spy on the staff's mobile devices and network systems, allegedly exploiting a vulnerability in the messaging service of a foreign smartphone brand. The centre generates, maintains, and broadcasts China's standard time. According to the State Security Ministry, serious breaches could have disrupted communication networks, financial systems, and critical infrastructure in China. The U.S. embassy in Beijing did not respond directly to the allegation but did assert in an email to *Reuters* that "China is the most active and persistent cyber threat to U.S. government, private-sector, and critical infrastructure networks." Cyber conflict has become a prominent element of global geopolitics and military and security-related competitions, including between the United States and China. Key advantages of cyberattacks include the ability to hold at risk important elements of national power and military readiness and to gain access to sensitive government information and commercial intellectual property with a lower degree of risk of attribution than more overt measures. Challenges associated with the attribution issue was demonstrated in reporting from *The Diplomat* about "what appears to be one of the most comprehensive known penetrations of South Korean government digital infrastructure in recent memory." Two independent security researchers uncovered the breach and published their findings in August through the hacker magazine Phrack. The leaked data shows access to South Korea's Onnara system, the government's operational platform that handles documents, inter-ministry communications, and knowledge management across central and local agencies. The breach also included compromised email credentials for multiple accounts at the Defence Counter-Intelligence Command and extends across multiple ministries, including the Ministries of Foreign Affairs and Unification. Attribution of the attack has been complicated. Compelling forensic evidence indicates the attacks originated from China rather than the North Korean government, which has frequently targeted South Korean government and military systems. Nonetheless, the originating location of the attacks may not reveal the full story behind the attack and why, and several theories of the responsible party have emerged. Some experts suggest that a Chinese hacking group was employed by North Korea or, plausibly, China and North Korea working together to carry out the attack. Others argued Russia might have employed the Chinese group while experts have also floated that the attack was a "sophisticated Chinese false flag operations designed to implicate North Korea while pursuing separate intelligence objectives." Ultimately, nations and militaries both large and small face growing cyber risks in which the level of threat has increased while the capability to carry out the attacks has diffused wide enough to make it difficult in many instances to definitely attribute—and therefore deter and respond to—who is ultimately responsible for the attack.

4. Human Protection and Performance

4.1	**And the award goes to . . .Singapore defence honours urban training facility** Singapore's SAFTI City training facility was awarded the country's Defence Technology Prize for helping to reshape how the Singapore Armed Forces (SAF) train for urban conflict (source and source) *Assessment:* The project was developed by ST Engineering with support from Singapore's Defence Science and Technology Agency (DSTA) and is focused on improving the realism of SAF training for urban combat, which is a growing area of emphasis for the city-state. Trainees at the technologically advanced facility can be equipped with laser-based systems to simulate tactical engagement and operate against mobile 3D targets that replicate a person's thermal signature for night-fighting training. Videos, smart instrumentation, and more than 10,000 sensors allow trainers to deploy interactive targets and deliver real-time feedback. SAFTI City features both low and high-rise buildings, multiple access points, interconnected structures, subterranean spaces, and an integrated transportation hub consisting of mock rapid transit platforms, a bus interchange, and an office complex. Other structures include a community centre, a school, malls, and hotels. It can host six company-level exercises with around 600 soldiers and up to two battalion-level missions with 1,200 troops. According to the Singaporean Ministry of Defence, the massive complex offers "a realistic environment to challenge our soldiers in the complexities of urban operations" with an emphasis on "the latest shifts in modern battlefield, such as the use of drones and robotics in urban environments."

Figure 5: A screenshot from a Singapore Armed Forces' video on SAFTI City. Source: Singapore Armed Forces

4.2	**Anduril wins contract to develop mixed-reality system for U.S. Army** Anduril announced it was awarded a $159 million contract for an initial prototyping period to develop a night vision and mixed reality system as part of the Army's Soldier Borne Mission Command program (source) *Assessment:* The previous DEFTECH Scan volume included a discussion of many of the priority areas of on-going development of night vision goggles (NVG). Among the persistent challenges with NVGs is that they, as Anduril noted in a press release, "provide sight, not perception." For example, current state-of-the-art NVG do not effectively fuse multiple spectral bands, integrate battlefield data, or enable soldiers to command robotic teammates directly from their display. The result is that "warfighters lose precious seconds just trying to get a common picture of the fight." The contract is designed to address this challenge with by fusing and interpreting data collected by NVGs and multiple sensors. On the hardware side, Anduril is collaborating with Meta, OSI, Qualcomm Technologies, and Gentex Corporation to develop a helmet-mounted mixed reality system that brings together advanced night vision with augmented reality overlays. The objective is to create a single perceptual layer that fuses day, night, and thermal imagery with real-time battlefield intelligence. The solution will be designed to be based on a modular component framework, allowing soldiers to tailor their loadout to their mission needs. The program's software architecture is based on Anduril's Lattice platform and incorporates an open software platform. Anduril reports that they have reduced over-the-air software update timelines by "99 percent", cutting the process from two days to just 15 minutes. This constitutes an important increase in capabilities for soldiers and also ensures heightened readiness of the equipment. Together, Anduril claims that the combination of hardware and agile software will "allow every soldier to see farther, know more, and act faster than ever before, redefining what it means to fight and win in the 21st century." The SBMC program was originally launched as the Integrated Visual Augmentation System (IVAS) program, which sought to customize Microsoft HoloLens goggles for military purposes. The program had several technical challenges and was criticized for its inability to solve these persistent challenges. In April 2025, the contract for IVAS was transferred from Microsoft to Anduril.

4.3	**Adapting to the end of the "Golden Hour"** Developments in Germany and the United States during the reporting period reveal one way militaries are responding to challenges associated with treating wounded soldiers in the age of persistent surveillance, drones, and targeting of medical personnel (source and source) *Assessment:* The prevalence of surveillance and strike drones in Ukraine has fundamentally changed battlefield medicine, especially as Russia prioritizes targeting medical personnel. Wounded soldiers can no longer be quickly triaged, treated, and evacuated to rear medical facilities for more extensive life-saving treatment, bringing an end to what militaries call the Golden Hour—the critical time period during which treatment greatly increases the odds of survival for wounded soldiers. At the same time, there are challenges in bringing more extensive critical care and resources, such as blood and oxygen, forward to the front line. Solving this issue requires several layers of innovative solutions, though the reporting period provided two examples of one way in which militaries are seeking to reform combat medicine efforts. On 15 October, Rheinmetall announced the German Armed Forces had awarded a €300 million contract to build armoured field hospitals. Deliveries will begin in 2029, with the hospital systems to be used by German forces stationed in Lithuania and other frontline deployments. Each hospital will include 11 armoured trucks equipped with medical containers that can stay attached while on the move, allowing for rapid deployment. The vehicles are based on Rheinmetall's HX military workhorse trucks, designed for difficult terrain and with added protection against attacks. Similarly, in October, U.S. company Valinor unveiled its Harbor system, a 20-foot shipping container that can be modified for different types of battlefield care, to include prolonged casualty care. The exterior can be hardened against ballistics and can be modified to power anti-drone defensive systems. Perhaps the most important feature of Harbor is the integration of modern information technology into battlefield medicine, such as sensors and connectivity that greatly improve medical outcomes in emergency triage situations. As Luke Sciulli, Valinor's head, told *Defense One,* "a big emphasis for us in building Harbor was the ability to do a lot of treatment remotely, including embedded telehealth, remote monitoring of various vitals, offline clinical resources . . . and even remote control of certain devices. . .It's about making it easier for clinicians and medics on the ground to do more with less."

Figure 6: A depiction of a Rheinmetall mobile field hospital. Source: Rheinmetall

5. Platforms and Weapons Systems

5.1	**The mighty Flamingo changes the calculus in the Ukraine war** The debut of Ukraine's first long-range, heavy payload domestically made missile could provide increased Ukrainian strategic autonomy as well as the capacity to strike deep into Russian territory (source and source) *Assessment:* Ukraine's armed forces have confirmed use of a long-range, precision-guided cruise missile capable of striking targets up to 3,000 kilometres away with a payload of up to 1,150 kilograms. The six-tonne system is six metres long, 1-metre in diameter, can travel close to the speed of sound, and can strike within 15 metres of an aiming point. The most high-profile use of the Flamingo (FP-5)—so named because the paint on a test copy turned pink—was a three-shot salvo against the relatively undefended Russian secret police base in North Crimea in August. Only two arrived on site, offering some insight into the accuracy of the Flamingo. Of those two, one missile missed the target by around 100-200 metres while the other "(levelled) a barracks and some hovercraft on a beach." As the *Kyiv Post* noted, "compared to the top-of-the-line US-made Tomahawk cruise missile, the Flamingo is less accurate but carries a warhead almost three times bigger." The cost is reportedly between $500,000 and $1,000,000 per copy. Ukraine has developed and effectively deployed drones such as the AN-196 Liutyi, AQ-400 Scythe, and FP-1. Western partners have also provided missile systems such as Storm Shadow, HIMARS, and ATACMS. However, all of these weapon systems are limited in range, while the Ukrainian drones are also slow and carry small payloads, minimizing their potential tactical and strategic impact. The manufacturer of the Flamingo, Ukrainian company Fire Point, has claimed that it can currently produce a missile per day (about 30 per month) with a longer-term vision to produce 2,500 per year with more funding. Even if this is an optimistic estimate, the fact that Ukraine is capable of domestically scaling the manufacturing a long-range "heavy hitter" cruise missile—even one that is less accurate and easier to intercept than higher-end cruise missiles—has the potential to change the situation in the Ukraine war. Notably, it increases Ukraine's strategic autonomy and ability to strike nearly any target deep into Russian territory, allowing the country to get around U.S. restrictions on targeting assets in Russia tied to weapons exports. Donald Hill, co-author of the Ukraine Update report, told *Kyiv Post* that "the FP-5 will likely be used to attack targets that other Ukrainian weapons cannot reach, penetrate, or damage to the same degree with smaller warheads. Being a local product, there are no restrictions on how it is used."

Figure 7: An image of the Flamengo FP-5 missile. Source: Fire Point via CEPA

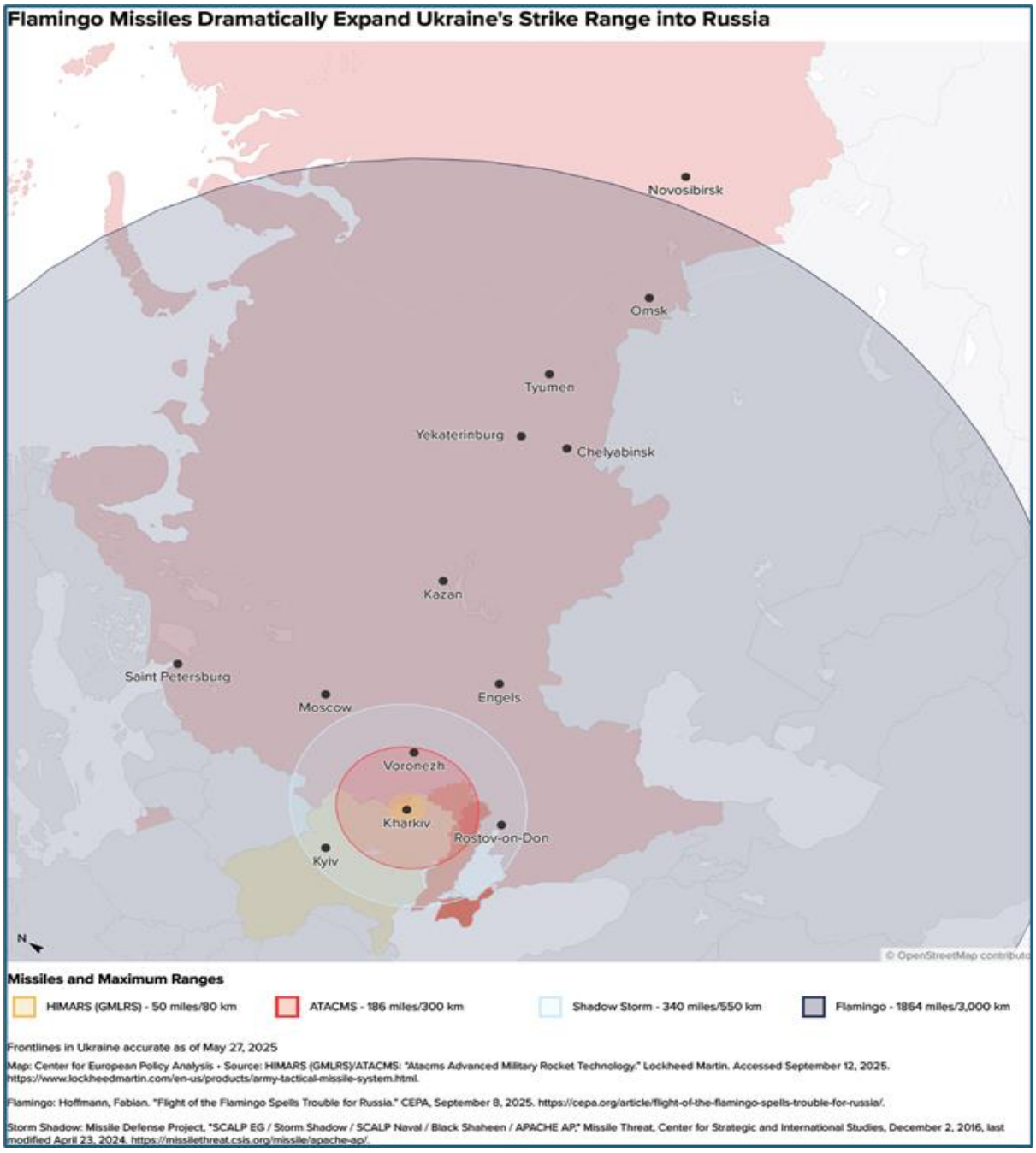

Figure 8: A map depicting the ranges of various Ukrainian weapons systems, demonstrating the greatly improved range of the Flamingo relative to ATACMS, HIMARS, and Shadow Storm. Source: CEPA

5.2	**Japan is entering the "counterstrike" era** A Japanese Aegis destroyer will be upgraded in the United States to be able to carry Tomahawk land attack cruise missiles as part of a January 2024 agreement between the United States and Japan for Japan's Self-Defence Force to acquire 400 Tomahawk missiles. (source) *Assessment:* The JS Chokai will undergo a year-long training and upgrade program to integrate the Tomahawk missiles. This is the first time a Japanese ship has been upgraded to carry Tomahawks, reinforcing the country's move away from a purely defensive and reactive defence posture to one that accommodates the concept of counterstrike. This allows Japan to strike weapons systems or bases attacking or posing an imminent threat to Japan from within other countries. As a result of the incorporation of the missiles, the Chokai's role will shift from an escort and area air and missile defence vessel to a distributed, sea-based, mobile strike asset able to hold at risk airbases, logistic hubs, and missile sites during a time of conflict. Japan is acquiring the latest Block V Tomahawk. The missile is a land-attack cruise missile that can be upgraded to a maritime strike variant, capable of engaging moving ships at a range of 1,000 miles. The Block V navigation system pairs GPS and INS guidance with terrain and scene-matching capabilities. The Chokai is already equipped with 90 strike-length Mk 41 vertical launch cells. These cells are usually outfitted with missile defence interceptors and surface-to-air missiles or anti-submarine weapons. These launchers are compatible with Tomahawk, which should speed integration. The vessel's crew will complete certification in crane operations, canister handling, and Tomahawk fire-control procedures. It will also cover strike mission planning, target route design, and in-flight re-tasking using the missile's two-way datalink.

5.3	**Flat Earth theory and the future of air power** On 20 October, Air Vice-Marshal James Beck delivered a speech on the future of UK air power at the Royal United Services Institute (RUSI). The speech laid out a compelling vision of how technologies are shaping existing and future challenges to air superiority and also described the capabilities required to overcome these challenges (source) *Assessment:* Vice-Marshal Beck stressed the importance of achieving air superiority from the outset of a conflict but also highlighted that actually achieving air superiority has become much more difficult due to the incorporation of new technologies and capabilities. Specifically, the proliferation of advanced radar systems, such as actively electronically scanned array (AESA) radar, has had an effect "tantamount to flattening of the earth," making tactics that relied on flying below radar coverage obsolete. Advanced sensors also enable detection ranges to increase from 100s to 1000s of nautical miles. In combination with the increased range and accuracy of surface-to-air and surface-to-surface missiles, air forces around the world are forced to change tactics and improve deep strike capabilities to achieve air superiority and establish deterrence. According to Marsh, "Deep Strike will become ever more challenging, but will become more critical to the success of an integrated campaign—unless you hold at risk what is most valuable to your adversary." In response to these challenges, the UK is investing in upgrading existing command and control capabilities to be "data-centric, cloud-based, and fully integrated across UK and NATO forces." The upgraded command and control will heavily incorporate AI "to enable machine-assisted decision-making, allowing commanders to act decisively at the speed of relevance." The UK will also invest in sensor technology to extend detection and tracking ranges. Further, Marsh stressed the importance of 6th Generation fighter aircraft, such as the Global Combat Aircraft Program featuring the UK, Japan, and Italy. Marsh observed that current 5th generation aircraft, like the F-35, will be the bare minimum required capability to operate effectively in the air combat environment of the future, characterized by increased anti-access/area denial capabilities. Indeed, Marsh draws an interesting comparison between 5th and 6th Generation aircraft, observing that "5th Generation is about tactical superiority" and "6th Generation is about bringing systems together that seek and understand the requirements and priorities for operational superiority." He also highlights three critical attributes required of the UK's future platforms, including extended range; a stealth signature that cannot be compromised and needs to be designed for future integrated air missile and defence systems; and the ability to carry meaningful payloads to maximize outcomes for the huge effort it will take to penetrate air and missile defence systems. Marsh's speech also focuses on the importance of being able to rapidly scale manufacturing and human capital. He concluded the speech by stressing the importance of air power in establishing and maintaining deterrence and serving as the UK Ministry of Defence's "first responder" in an uncertain world.


deftech.ch