Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

DEFTECH-SCAN

December 2025

OTH INTELLIGENCE GROUP

deftech.ch/scans

Dear Reader,

First of all, we would like to wish you a wonderful 2026, which started pretty strong already!

A key feature of the Deftech-scans is the systematic use of sources and links, and we wanted to offer the ability to connect information across multiple documents.

We have addressed this by implementing a new document storage system and a powerful search engine that links insights across all Deftech-scans and a broader documents corpus. While integrating an AI was an option, we chose to work directly with original documents for cost and energy reasons. Further insights into this strategy are available here (in French, but easily translatable using AI tools - smile).

As we prepare for what's next, here are the key updates

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	**Limitations and advantages of AI autonomy in Ukraine** An early December article from an AI autonomy entrepreneur and expert revealed how autonomy is impacting the battlefield in Ukraine while also highlighting persistent challenges and a vision for the future of AI autonomy for Western militaries. (source) *Assessment:* On 2 December, entrepreneur Vitaliy Goncharuk published a Substack article that reviewed the effects of AI autonomy on the conflict in Ukraine. Goncharuk is the head of A19Lab, a company developing AI-autonomous systems for drones and robots. He also served as the chair of Ukraine's AI Committee from 2019 to 2023. The article begins by identifying the tasks AI is currently supporting or enhancing in Ukraine, including last-mile target guidance, target recognition, GPS-free visual terrain navigation—a capability that is highly valued in Ukraine's dense electronic warfare environment—route planning, and swarm coordination. While AI has been helpful in each of these functions, its impact has been moderated by technological realities and data quality. For example, the author asserts that most of the AI autonomy capabilities deployed in Ukraine are "built on 'low tech' foundations—often open-source software and cheap hardware." The upside of this model is that innovation occurs at low cost. However, the trade-off is that significant breakthroughs in capabilities are rare and innovation is frequently more incremental. The second limitation for AI in Ukraine has been data. Tremendous amounts of data have been collected over nearly four years of conflict. This data has helped Ukraine build more robust and effective algorithms. However, the article identifies three caveats about the collected data. First, the quality of the data is mixed. Much of it is low-resolution analogue feed and is not necessarily useful for making higher-end discriminations between, for example, a Ukrainian soldier and a Russian one. Second, it takes time to efficiently label and process data and for training pipelines to make use of it. Third, the value of data is context dependent, making it "invaluable for Ukraine's current fight" and providing Western militaries "insight into modern high-intensity warfare" but still "not a silver bullet for all future AI needs." The analysis concludes by looking at the future of AI autonomy development. Goncharuk argues that for the next generation of drones capable of deep strike operations at ranges of 200-400 km, "drone autonomy will have to leap to a whole new level." Sophisticated guidance systems—scene matching, predictive course adjustment, threat avoidance, and perhaps even the ability to pick among pre-vetted targets autonomously if the drone loses contact—will be required to allow drones to travel faster and further, similar to cruise missiles. An additional key takeaway for Western militaries is for them to begin to collect "imagery and sensor data on whatever systems a potential opponent might use, and to train AI on that *before* any war starts."

1.2	**AI to speed up submarine maintenance** The United States Navy agreed to a contract with Palantir Technologies to use AI tools to manage the submarine industrial base supply chain in an effort to reduce maintenance downtime (source and source) *Assessment:* The contract, valued at $448 million, is part of the Navy's Ship Operating System (Ship OS) effort. This initiative seeks to incorporate AI and other software tools to accelerate shipbuilding and maintenance processes. Palantir's Foundry and Artificial Intelligence Platform has already been tested in pilot programs across submarine shipyards. According to *Business Insider*, at General Dynamics Electric Boat shipyard, submarine schedule planning was reduced from 160 manual hours to under 10 minutes using the tool. Portsmouth Naval Shipyard saw material review times for submarines reduce from weeks to under an hour. The recently announced contract to expand application of Palantir's AI tools will focus on providing more visibility into the submarine supply chain. The software will be used to replace workers needed to manually track parts using spreadsheets and better predict when parts are needed. Palantir CEO Alex Karp claimed that the software provides "predictive analytics to understand when we're going to potentially have problems in the supply chain. Rather than hearing about a problem that day that will stop [submarine maintenance], we will know 60,90, 120, 180 days in advance that we've got it." If successful, the application of AI and predictive analytics at scale to the submarine industrial base and broader maritime industrial base could help address a significant challenge for the U.S. Navy as well as other navies throughout the world. Bryan Clark, a naval expert and senior fellow at the Hudson Institute in Washington, D.C., told the *Wall Street Journal* that "the Navy's public shipyards have been terrible at the management process in general and they're extremely inefficient. There's a lot of dead time where submarines are just waiting because the right people and the material are not in the right place at the right time to start the job when they were supposed to start the job."

1.3	**Crossing the threshold: Anthropic detects first large-scale, coordinated cyber-espionage operation executed primarily by AI** An Anthropic report accuses a Chinese-backed threat group of using AI to manipulate the company's generative AI tool, Claude Code, to carry out espionage-focused attacks against roughly 30 entities across the United States and allied nations (source and source) *Assessment:* The report entitled "Disrupting the first reported AI-orchestrated cyber espionage campaign" details the sophisticated campaign, acknowledging "a handful of successful intrusions" into "major technology corporations and government agencies." It also claims the attack "marks the first documented case of agentic AI successfully obtaining access to confirmed high-value targets for intelligence collection" and suggests that AI-enabled cyber capabilities have developed more quickly than expected. Anthropic claims it detected the attack in mid-September 2025, assessing with "high confidence that it was conducted by a Chinese state-sponsored group", designated GTG-1002. The report also describes the attack as demonstrating "unprecedented integration and autonomy of AI throughout the lifecycle, with the threat actor manipulating Claude Code to support reconnaissance, vulnerability discovery, exploitation, lateral movement, credential harvesting, data analysis, and exfiltration operations largely autonomously." Approximately 80-90% of the tactical operations were carried out by AI independently, greatly accelerating the rate at which these attacks were carried out in comparison to an attack carried out largely by human operators. The human attackers that unleashed the automated attacks were able to circumvent Claude's safety systems through social engineering, convincing Anthropic's AI that they were legitimate cybersecurity professionals conducting authorized testing. According to the *Wall Street Journal* "By presenting malicious tasks as routine security work, they manipulated Claude into executing attack components without recognizing the broader hostile context." The attack represents a significant advancement in cyber-attack operations. Notably, it signals an evolving move away from cutting-edge, human-crafted malware or expensive proprietary tools to the use of widely available technology—or as one commentary on the attack assessed, moving from the "craftsman" to "the assembly line." Anthropic, which voluntarily released the details of the attack and its response, argues that "the techniques we are describing today will proliferate across the threat landscape." This development places a premium on security teams experimenting with applying AI defence to counter AI cyber-attacks as well as sharing of threat data, improved detection methods, and stronger safety controls across the AI and cyber community.

2. Robotics and Autonomous Systems

2.1	**Man's best friend: PLA exercise uses robot dogs to lead amphibious assault** Footage shown on Chinese state television network CCTV showed "robot wolves" deployed as the first wave of an amphibious assault as part of an exercise to develop and refine new concepts of crewed-uncrewed teaming operations (source) *Assessment:* One of the most frequently referenced benefits of uncrewed systems is that they reduce risk to human operators by carrying out dirty and dangerous tasks. Few tasks are more dangerous than amphibious landings against armed and entrenched positions. In a recent exercise, the PLA used robot dogs in a similar way to drone swarms to clear barbed wire and other obstacles as part of an amphibious assault against a prepared and fixed position. A report from Singapore-based news site *Think China* relayed that "what was the most dangerous 200 metres that soldiers risked their lives to breach is now accomplished by 'wolfpacks.'" The exercise comes at a sensitive time in the region, as concerns about potential PLA military action against Taiwan are on the rise. Of course, as with nearly all new technologies and operational concepts, some challenges can limit the utility of robot dogs/wolves in combat or extended deployment. Lt. Colonel Jahara "Franky" Matisek, a U.S. Air Force command pilot and command centre director with the U.S. Northern Command, told *The Independent* that these systems "are suited for urban reconnaissance, breaching, or remote weapons but are limited by battery life, vulnerable communications, and small payloads." Furthermore, their value "hinges on robust sensors and secure networks", potentially making them "too niche" for open-field charges. Nonetheless, continued testing and development of these ground robots are likely to deliver more advanced capabilities and be more prominently incorporated over time into human-machine teams to accomplish dangerous missions.

Figure 1: A screenshot from CCTV showing the 'robot wolves' operating in sandy surroundings during a Chinese military exercise. (source: CCTV via The Independent)

2.2	**Convergence and dispersion: the threat of jihadist use of homemade drones** The *Militant Wire* Substack published an informative investigation of how the convergence and proliferation of 3D printing and, especially, commercial drone capabilities are driving an intensified drone threat to Western infrastructure and populations from jihadist groups (source) *Assessment:* The paper begins by describing a recently uncovered and disrupted plot to assassinate Belgian Prime Minister Bart De Wever, among other politicians. The plot featured the use of kamikaze drones that included parts printed with 3D printers. The article's authors assert that proliferation of commercial drones, more capable 3D printers, and the accessibility of instructional materials required to operate printers and weaponize drones marks a "significant shift in how terrorists employ advanced tools, reinforcing the urgent need for heightened vigilance and strategic responses to this emerging threat." The analysis traces the recent history of jihadist groups' focus on the use of "do-it-yourself" type weapons, including explosives, as well as efforts to incorporate drones for surveillance, propaganda, and, eventually, strikes in conflicts in the Middle East. While drones have been effectively deployed in Syria and Iraq in the last decade plus, the authors note that "no successful jihadist-inspired drone attacks have occurred in Western countries." However, there have been "multiple directed, facilitated, and inspired plots in the United States and Europe" involving drone technology that have been disrupted. The challenge of disrupting jihadist supply chains is complicated by a growing trend of these groups leveraging organized crime networks to procure drones in Europe. The article cites two recent examples. One occurred in Denmark in 2023 and the second involved a Europe-wide plot in 2024 and 2025 that spanned Spain, Germany, France, and the United Kingdom. In both incidents, Hamas and Hezbollah networks used individuals in criminal organizations to acquire drones for terrorist attacks. The authors ultimately call for "immediate action" to disrupt this type of attack including disrupting supply chains. They also advocate for allocating "additional resources to disrupt terrorist use of the internet and improve content takedown processes across small and large platforms" to reduce access to the instructional and inspirational material that is helping drive and facilitate this threat.

2.3	**Sub Sea Baby: Ukraine claims first underwater drone attack on submarine** On 15 December, the Ukrainian state security service (SBU) claimed to have carried out the first-ever uncrewed underwater vehicle (UUV) attack on a Russian naval vessel (source and source) *Assessment:* The strike allegedly damaged a Project 636 *Varshavyanka* class diesel-electric submarine (also known as *Improved Kilo* class) in the Black Sea base of Novorossiysk. The extent of the damage inflicted on the sub has been difficult to determine, though commercially-available satellite imagery of the base reveals extensive damage to a nearby dock. Russia denied that the attack did significant damage, noting that "not a single ship or submarine, as well as the crews of the Black Sea Fleet stationed in the bay of Novorossiysk naval base, were damaged as a result of the sabotage." The attack was revealed in a statement accompanied by a video of the strike. The video includes approximately 15 seconds of video at the base with several Russian military vessels outlined in green boxes. At 16 seconds, a large explosion occurs on the left side of the video. Ukraine claims that this was the UUV, known as Sub Sea Baby, striking the Russian submarine. Ukraine has previously used uncrewed surface vehicles (USVs) to strike Russian naval assets as well as infrastructure such as bridges and bases. While Ukraine has employed UUVs in military operations in the past, they have been used in undersea surveillance and reconnaissance and mine hunting roles. This attack would constitute the first known time that Ukraine or any other nation has used UUVs in a maritime strike role.

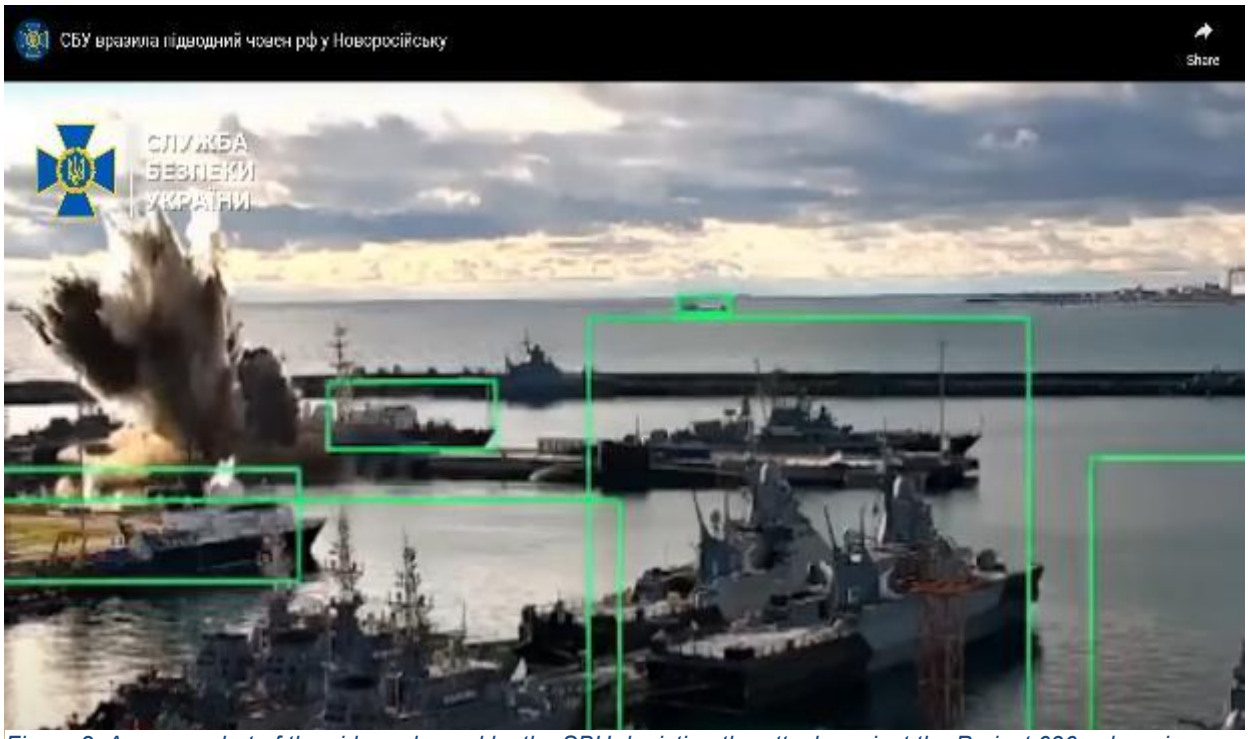

Figure 2: A screen shot of the video released by the SBU depicting the attack against the Project 636 submarine. Source: SBU

3. Connectivity

3.1	**Cars, boats, & buses: novel technology and new attack vectors of hybrid warfare** Two incidents during the reporting period demonstrate how new commercial technologies are opening up vulnerabilities for civil infrastructure and, as a result, societal and political stability in Europe (source and source) *Assessment:* During a public transportation conference in November, representatives of Oslo's public transport authority, Ruter, confirmed that the city's Chinese-made buses could, in theory, be remotely disabled using the control system for the battery. The findings emerged from a test involving driving an electric bus into a decommissioned mine inside a mountain. The remote, rocky location limited digital interference, making it more difficult to gain access to the bus's operating system. Yet, Ruter still found the bus was vulnerable to sabotage. The findings have confirmed growing concerns in several European countries about the risks associated with incorporating Chinese-made vehicles and infrastructure, including solar panels and 5G connectivity. British lawmaker Alicia Kearns released a statement on 19 November warning of the risks of using Chinese-made equipment, saying that "Norway and Denmark alerted us to the existence of dual-use kill switches in Chinese-made electric buses. These switches allow China to switch off buses and bring chaos to transport systems." Low-cost Chinese-made solar panels have also come under scrutiny. Roughly 30 members of the European Parliament wrote to Europe's top cybersecurity and energy officials in October to warn that inverters—devices that hook solar panels up to the broader electrical grid—could be exploited to disrupt the power system. For its part, the Chinese government has strenuously denied the risks associated with the adoption of Chinese-made vehicles and solar panels. Beijing's embassy in Norway noted that "overstretching the concept of security only ends up hindering competition and innovation, rather than blocking risks." In a separate incident, Italian authorities warned France's General Directorate of Internal Security that software used by cybercriminals may have infected computer systems aboard the Italian-owned *Fantastic* ferry docked in the French Mediterranean port of Sete. The remote access trojan (RAT) software allows users to control computer systems remotely and could have been used to take control of the ferry's computers. A Latvian crew member has been arrested. The French prosecutor's office released a statement saying that attack was the result of foreign interference and was launched "by an organized group to attack an automated data-processing system, with the aim of serving the interests of a foreign power." More on the growing concern in Europe about Russian hybrid warfare is discussed in the final two entries of the Platform and Weapons Systems section of this report.

4. Human Protection and Performance

4.1	**Ukrainian training system pits individual drone and counter-drone operators in virtual duels** The system merges first person view (FPV) drone control, real-world physics, and data-driven analytics to deliver realistic combat training for both drone and counter-drone operators (source) *Assessment:* Ukrainian engineering company Atmaraksi has developed a VR simulation system called Duel that pits first-person view drone operators against counter-drone shooters in digital training duels. The system places soldiers in high-pressure scenarios where they are forced to make quick decisions—take cover or stay in the fight, for example. Duel reportedly recreates the physics and logic of real-world combat in an environment where instructors can swap locations, weapon systems, and specific drones depending on the desired training objectives. Instructors also benefit from performance logs and associated analytics, allowing them to evaluate and refine training programs and customize programmes for individual operators. The system's reveal underscores several consistent themes of past DEFTECH scan volumes: • Increased adoption of virtual and augmented reality (V/AR) as a means of reducing costs and timelines associated with training. These systems also provide flexible and customizable training environments that allow operators to experience and prepare for more battlefield scenarios. • The complexity and importance of the drone/counter-drone conflict and competition. Training both drone and counter-drone operators in a single competitive and dynamic training environment offers an efficient opportunity to improve the skill set of both offensive and defensive operators. • A pivot toward adopting proven and commercially mature solutions that can be adapted for several different training applications. Atmaraksi has successfully developed VR solutions for both defence and civilian sectors, including developing a VR rehabilitation program to help patients and military personnel recover from phantom pain and post-traumatic stress disorder.

Figure 3: A screenshot from an Atmaraksi YouTube promotional video for Duel. The image depicts a counter-drone operator using the Duel VR headset and one of the associated weapons to engage a VR drone Source: Atmaraksi, via NextGen Defense

4.2	**People's Liberation Army (PLA) seeks to counter dirty bomb radiation** Researchers with the PLA Joint Logistic Support Force (JLSF) University of Engineering in conjunction with the PLA's Rocket Force Research Institute published a study that explores how an airborne weather modification system could trap and contain radioactive clouds within minutes of the explosion of a dirty bomb (source (firewalled) and source) *Assessment:* A dirty bomb pairs radioactive material with explosives. When detonated, these weapons disperse radiation over a wide area. The resulting cloud of radiation contaminates the surrounding air, putting people and infrastructure at great risk of long-term damage. The PLA's experimental "high-altitude rapid-response suppression" system would launch a payload shortly after detonation of a dirty bomb. The system would then release special chemical agents that attach to radioactive particles, making them heavier and bringing them to the ground. Lin Yuanye, a nuclear emergency expert with the JLSF and study team lead, wrote that "by releasing suppression agents that interact with radioactive aerosols through mechanisms such as adsorption (the process through which atoms or molecules stick to surfaces), clustering, and coagulation, these systems can significantly accelerate the in situ or near-source deposition of hazardous particles." The team ran a series of "high-fidelity computer simulations" as well as controlled tests in a real-world environment. The real-world test involved an explosion on a hard concrete surface, designed to mimic urban infrastructure. Of course, no actual radioactive material was used in the explosion, though the researchers did employ tracer dyes—non-radioactive substances that behave like radiation—to simulate the spread of a radioactive cloud. A high-altitude balloon, laser rangefinders, and angle-measuring instruments were used to collect data while specialized software processed data on how the cloud moved and expanded. The simulation found that if left unchecked, a single dirty bomb could create a radioactive contamination zone covering nearly 10 sq. km, a significant area, especially in an urban environment. To counter this spread, researchers proposed rocket-launched suppression systems that carry special suppression agents into the upper atmosphere within a handful of minutes of the explosion. The challenge is getting the suppression chemicals into the radioactive cloud quickly. Researchers found that to achieve 90 percent suppression of radioactive fallout, the rockets must launch within about two minutes of the explosion, placing a premium on readiness, early warning, and detection.

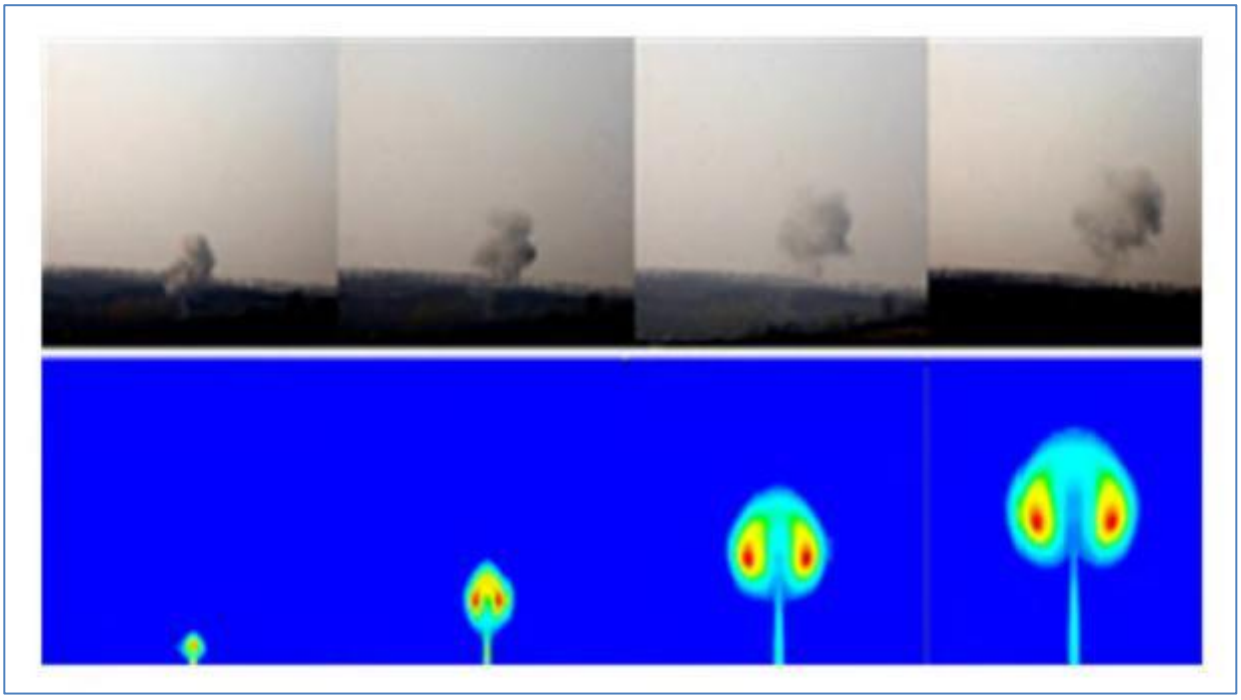

Figure 4: A simulated "dirty bomb" attack produces a cloud in a PLA field test. Photo: Joint Logistic Support Force University of Engineering, Rocket Force Research Institute via South China Morning Post

5. Platforms and Weapons Systems

5.1	**Poland chooses SAAB's fifth generation sub to replace Soviet-era vessels** The Polish government announced it has selected SAAB's A26 Blekinge-class submarine to replace its existing Kilo-class vessel. The A26 is billed as the first fifth-generation submarine, outfitted with a range of advanced technologies and capabilities to allow it to stealthily carry out multiple mission sets (source and source) *Assessment:* The contract is expected to be signed by mid-2026 with the first ship to be delivered by 2030. The total contract value is expected to be around 10 billion zlotys ($2.74 billion), but some observers believe it could increase to 36 billion zlotys ($9.8 billion). The A26 brings impressive capabilities designed to align with NATO's growing focus on Multi-Domain Operations (MDO) and multi-role platforms and systems. Among A26's characteristics that differentiate it as a fifth-generation vessel are: • Signature reduction: Balanced multi-domain signatures and "cutting-edge signature management" make the sub extremely difficult to detect. This is achieved through special coatings and hull design that minimize radar, visual, and IR surface signatures and through Saab's patented Stirling-Air Independent Propulsion (AIP), which allows the A26 to stay underwater for longer periods of time before needing to surface. • Seabed warfare and multi-mission operations: Uncrewed underwater vehicles (UUV) delivery systems allow it to carry out seabed warfare missions while also carrying out intelligence, surveillance, and reconnaissance (ISR), and long-range strike missions. • Information warfare: The A26 can support information warfare efforts by gathering and exploiting enemy communication and electronic signals, providing valuable insights into adversary intentions and capabilities. Stopping signals and disrupting communications are part of this enhanced mission set. • Multi-Domain Operations: The submarine meets the requirements of NATO's Multi-Domain Operations (MDO), an important selling point for the Polish government, allowing it to support the coordination and combination of single, simultaneous, or sequential actions across various domains at speed and at scale.

Figure 5: A 2020 rendering by naval analyst HI Sutton of the A-26 sub and many of its distinguishing capabilities. Source: HI Sutton, Forbes

5.2	**Jane's assesses China's enhanced anti-access/area denial (A2/AD) posture in the Indo-Pacific** The free access article profiles four high-speed anti-ship missiles that were displayed during the 3 September PLA military parade commemorating the 80th anniversary of the end of the Second World War (source) *Assessment:* The new series of anti-ship missiles "likely offer greater speed and precision than previous generations of similar weapons," according to the defence intelligence company. Janes analysts note that together these missiles constitute "a significant advancement in China's maritime strike capabilities." • YJ-15: The extended-range supersonic missile is designed to engage high-value naval targets such as aircraft carriers and large surface combatants. Its supersonic speed and ability to execute evasive manoeuvres during the terminal phase reduce reaction times for adversary defence systems, complicating interception. The missile is also designed to be launched from H-6 strategic bombers, increasing the range of the system. It may also have a secondary land attack role. • YJ-17: This hypersonic weapon's design suggests it can withstand temperatures associated with flights that occur between Mach 5 and Mach 8. The lack of visible air intakes indicates that the YJ-17 does not employ air-breathing propulsions such as scramjets as some hypersonic weapons do. Rather, it is a boost-glide weapon that relies on a solid-fuel booster for its initial acceleration before moving into an unpowered glide phase. Its size also indicates compatibility with naval vertical launch systems as well external carriage by H-6 bombers, making it a flexible system that could be integrated into multiple platforms. • YJ-19: The Y-19 is a hypersonic weapon that incorporates a scramjet engine to reach estimated speeds between Mach 5 – Mach 10 with a range of approximately 500 km. Given peculiarities of the missile's design, *Janes* assesses that the PLA Navy (PLAN) conceived the missile to "provide the PLAN with a hypersonic missile that is endowed with the stealth advantages associated with submarine deployments." Combining stealth deployment and launch with the high speeds of hypersonic weapons will create new challenges for air and missile defence capabilities across the region. • YJ-20: The JY-20 is large missile with substantial payload capacity, suggesting it is a strategic weapon. The missile is a hypersonic weapon that likely will travel between Mach 6 and Mach 7 during cruise with terminal velocities potentially reaching Mach 9. It has a range of 1,500 to 2,000 km, enabling deep strike across the Indo-Pacific region Images and Janes analysis of missile design attributes are included in the figure below.

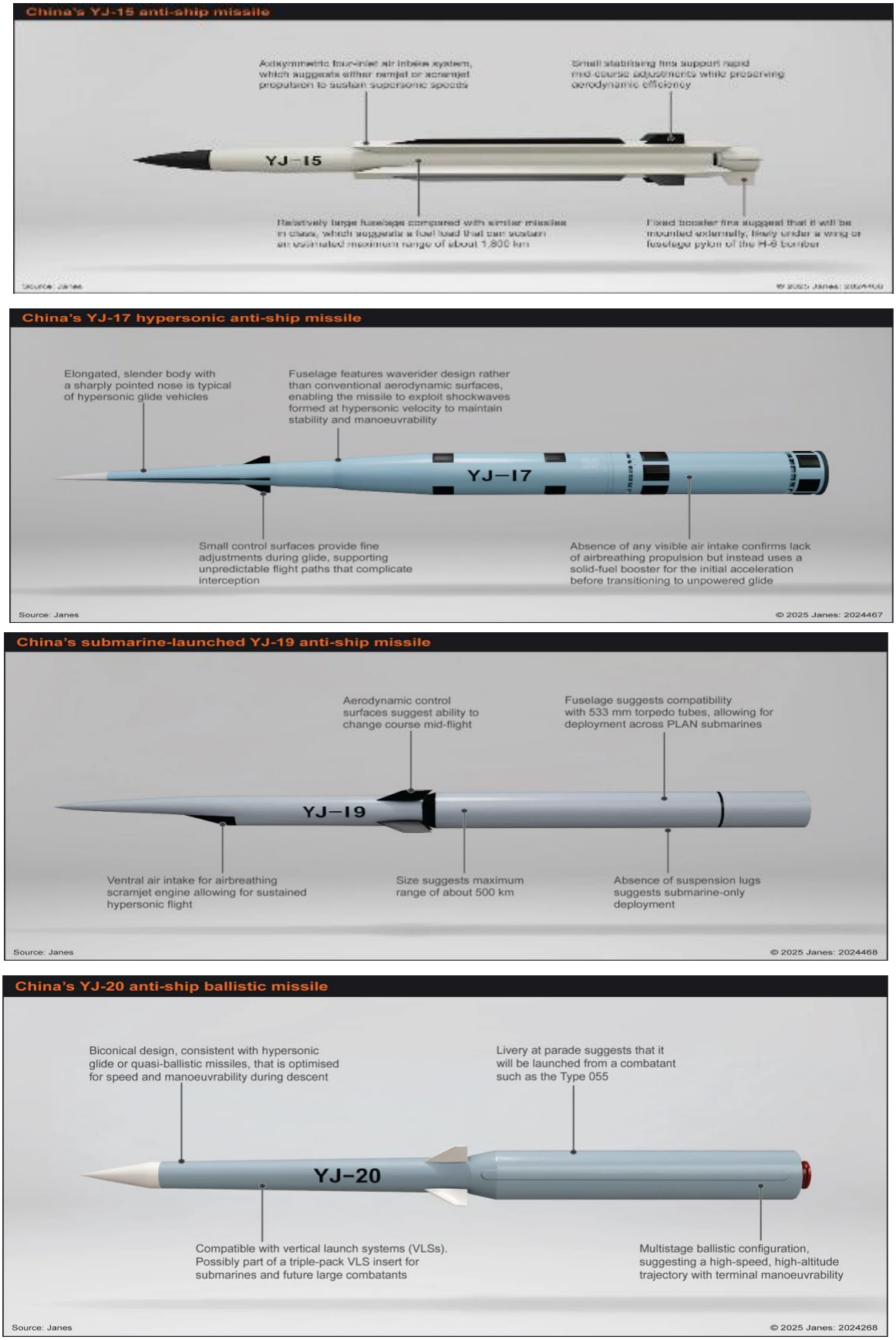

Figure 6: Janes images and analysis of the four missiles described in the text above. Source: Janes

5.3	**Battlestar Galactica: coming to a Southeast Asian strait near you!** Singapore launched a new class of six Multi-Role Combat Vessels (MRCV). The country's defence minister, Chan Chun Sing, likened the new vessel to capabilities in sci-fi programs and movies such as "Battlestar Galactica" (source and source) *Assessment:* Singapore launched the *Victory*, the first of a class of six MRCVs to replace older ships and bring more flexible, upgradable, customizable, and advanced capabilities to the fleet. The ships will eventually replace the six Victory-class missile corvettes beginning in 2028. The new vessels are designed to be motherships capable of carrying a wide range of types of capabilities and payloads. The initial ship in the class features eight containerised modules allowing it to carry out various missions. Chan announced the new ship will "bring together unmanned air capabilities, unmanned surface capabilities, and unmanned subsurface capabilities" in an effort to meet the growing range of threats to Singapore's national security. He also compared the new class of vessel to a mothership in the sci-fi TV show Battlestar Galactica that is integrated with artificial intelligence and an "evolving brain" able to control the assets under its charge and network with a larger fighting force, operating as part of a system of systems. The new class of ships is being built by ST Engineering with Swedish firm Saab Kockums providing the vessels' composite superstructures. The ship is also co-developed by Denmark's Odense Maritime Technology. The *Victory* will now undergo outfitting, platform and combat systems integration, and acceptance trials. In addition to its novel role as a mothership, the Victory is also distinguished by other advanced capabilities such as a composite structure, multi-function radar, multiple launch and recovery systems for crewed and uncrewed vessels, an integrated full electric propulsion system, dedicated missile systems and gunnery, advanced sensors, cyber defence, and on-board training simulators (see image below).

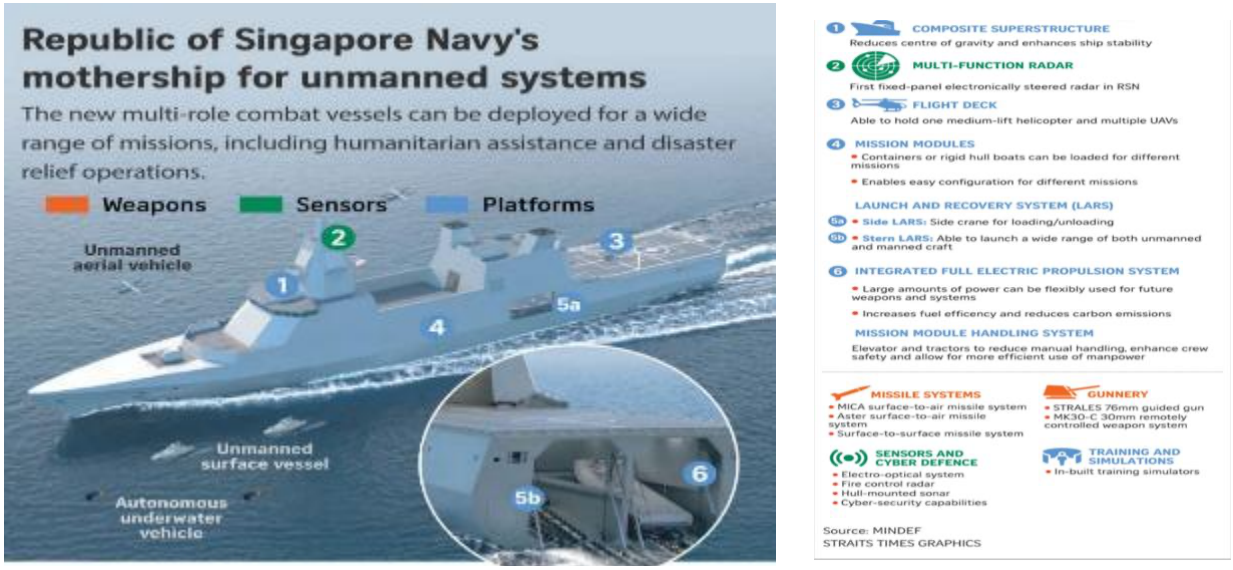

Figure 7: A rendering of the Victory-class mothership and associated description of relevant capabilities. Source: Singapore Straits Times

5.4	**Another laser incident, reinforcing UK and European concern over Russian hybrid activity** On 19 November, the UK revealed that a Russian ship used a laser to disrupt Royal Air Force (RAF) pilots tracking activity near UK waters. The "deeply dangerous" move escalated tensions between the UK and Russia as Russia continues its "shadow warfare" in the region (source and source) *Assessment:* While this was the first time a Russian ship has been accused of using lasers to blind UK military pilots, previous volumes of this report have cited numerous other examples of China, in particular, using directed energy weapons to carry out these provocative attacks. The incident took place as RAF Poseidon P-8 planes and a UK frigate were following the Russian ship, *Yantar*. Defence Secretary John Healey claimed that the UK has changed its rules of engagement to allow UK forces to follow the *Yantar* more closely "when it is in our wider waters." Healy also told the media that the UK has "military options ready" should the *Yantar* engage in similar behaviour in the future. On 6 November, the Dutch Navy announced that two of its vessels escorted the *Yantar* out of the North Sea, where it was operating near Dutch territorial waters. Russia has denied the incident and has called on the British government "to hold off taking any destructive steps which might aggravate the crisis situation on the European continent." The incident takes place as concerns over Russia's growing grey zone activities are on the rise in much of Europe. On the same day as the UK MoD announced the laser attack, the Center for European Policy Analysis (CEPA) released a report entitled "War Without End: Russia's Shadow Warfare" that diagnoses the dimensions of the shadow war challenge and identifies the organisations and individuals playing a prominent role in the execution of this shadow war. The report's opening statement provides some insight into the challenge: "Severed cables. Disrupted aviation. Arson. Sabotage. Assassination. Infiltration. Attacks designed to distract, to confuse, and to dismay an adversary—but not to provoke a response. Such is shadow warfare, causing damage and costing lives but operating below the traditional threshold of warfare." The CEPA report's release follows an August 2025 report from the *International Institute for Strategic Studies* (IISS) entitled "The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure." According to the report, "through its campaign of sabotage, vandalism, espionage, and covert action, Russia's aim has been to destabilise European governments, undermine public support for Ukraine by imposing social and economic costs on Europe, and weaken the collective ability of NATO and the European Union to respond to Russian aggression." Emerging technologies such as the use of uncrewed systems for espionage and GPS jamming are specifically cited in the report.

5.5	**The UK's Atlantic Bastion moves forward** On 8 December, the UK Royal Navy (RN) provided updates on the progress of its Atlantic Bastion concept. The concept was developed to deter an detect some of the threats discussed above, specifically, increased Russian submarine activity in the North Atlantic and North Sea and threats to the UK's critical undersea infrastructure in the area (source and source) *Assessment:* Atlantic Bastion was initially revealed in the government's Strategic Defence Review, released in June 2025.The concept involves a rethinking of the RN's force structure with a focus on developing a hybrid force to defend the UK and allies against evolving maritime threats. This force will include a combination of autonomous uncrewed systems and crewed platforms, which will be paired with novel advanced sensors and a "cutting-edge digital infrastructure" to better detect and deter Russian undersea activity in the North Atlantic. According to the UK Ministry of Defence (MoD), "Atlantic Bastion places the UK at the forefront of a technological revolution in naval warfare." Updates on the program were provided through two linked efforts on 8 December. First, a UK Ministry of Defence (MoD) press release revealed that a combined MoD/industry initial investment of £14 million has been established for testing and development. Twenty companies "are already showcasing technology demonstrators, with public investment matched by private investment so far at a 4:1 ratio." These firms range from defence primes to established defence technology players and small and medium sized enterprises. The press release included quotes from representatives of Anduril UK, BAE Systems Defence Solutions, and defence AI and software company Helsing. The press release was followed by a speech by First Sea Lord General Gwyn Jenkins at the International Sea Power Conference. The First Sea Lord hailed Atlantic Bastion as an "innovative concept of connecting autonomous sensors in the Atlantic [to] be our 'eyes and ears.'" Luke Pollard, UK Minister for Defence Readiness and Industry, also gave a keynote speech at the conference, telling participants that "Atlantic Bastion is an important step towards a hybrid RN, where an artificial intelligence-powered shield of sensors, autonomous vehicles, and traditional naval and air assets come together." Also in December, the Royal United Services Institute (RUSI) released a report entitled "The Atlantic Bastion" that assesses the probable deterrent effect of the concept. Ultimately, the paper endorses the concept but also highlights that "there is a risk that the Royal Navy defines the Atlantic Bastion too narrowly: as a network of relatively low-mobility sensors in the Norwegian Sea." The authors recommend extending the geographical scope westward into the Atlantic and eastward into the Barents Sea. They also recommend incorporating long-range, non-US strike capabilities and integrating naval mining and uncrewed underwater vehicle (UUV)-delivered loitering munitions into the Bastion architecture to enhance its deterrent value.

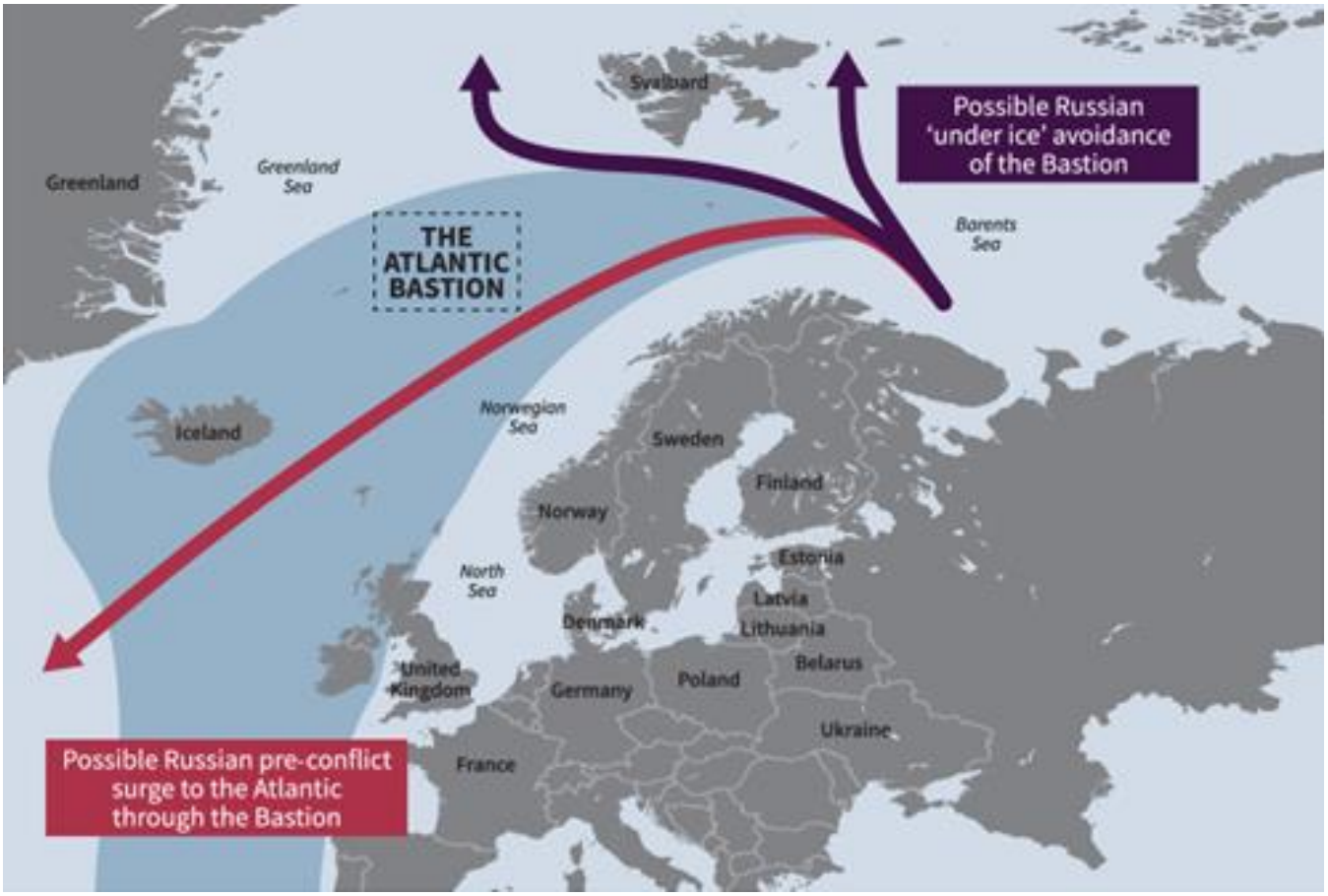

Figure 7: A map visualising the scope of Atlantic Bastion and potential Russian actions and counteractions to circumvent the concept. Source: [RUSI, Sidharth Kaushal, and Edward Black]

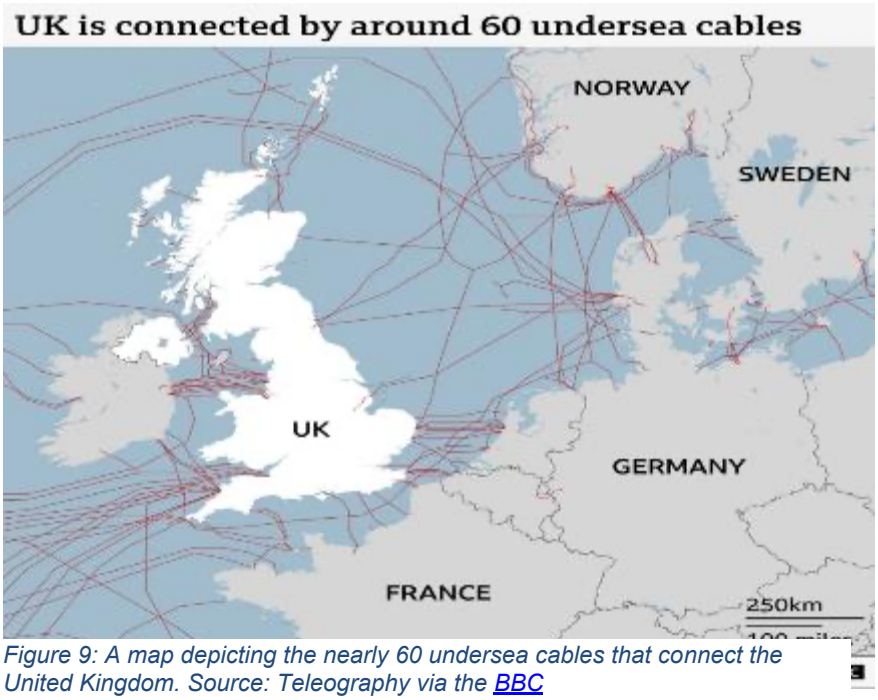

Figure 9: A map depicting the nearly 60 undersea cables that connect the United Kingdom. Source: Teleography via the [BBC]

6. Manufacturing and Industry

6.1	**The "War Unicorns": venture capital and the future of the defence industrial base** Recent focus of the U.S. Department of Defense (DoD) on reshaping defence acquisition to accelerate the development and adoption of advanced capabilities has drawn attention to the growing presence of venture-backed defence companies and the changing nature of the U.S. defence industrial base (source, source) *Assessment:* In a 20 November post entitled "The War Unicorns", the U.S. Defense Tech and Acquisition Substack profiled 21 defence tech unicorns with over $1 billion in valuation that are "powering tomorrow's arsenal" in the United States. According to the authors, these companies are "rewriting the rules of modern warfare, blending Silicon Valley speed and tech with battlefield grit" and delivering capability at pace across the following six categories of capabilities: • AI and autonomy (10): Palantir Technologies, Anduril Industries, Saronic Technologies, Shield AI, Skydio, Applied Intuition, Scale, Govini, Vannevar Labs, Rebellion Defense • Directed energy and counter UAS (1): Epirus • Space launch (5): SpaceX, Blue Origin, Firefly Aerospace, Apex, Relativity Space • Space systems and intelligence (3): Hawkeye360, Planet, Sierra Space • Manufacturing (1): Divergent Technology • Quantum (1): PsiQuantum Several commentators both within and outside of the U.S. DoD have noted that this focus on speed, agility, modular and open architectures solutions, software, and more fluid and iterative development has created a significant cultural and operational challenge for the U.S. defence community and the traditional industry primes that have supported it. The need to address these challenges was at the heart of the DoD's "Acquisition Transformation Strategy", released on 7 November. The document outlines the ways in which the DoD will transform the U.S.'s "antiquated acquisition processes" and revitalize "the atrophied Defense Industrial Base (DIB) by prioritizing speed, flexibility, and rigorous execution." Among the key thrusts of the document is the need to engage more effectively with the commercial industrial base and new, more dynamic providers, moving away from a sole reliance on a small group of primes. The document notes that large DoD programs too frequently go over scheduled development timelines and budgets. The strategy rests on several key initiatives: 1) Fuel the Arsenal of Freedom: Rebuild the DIB; 2) Elevate and Empower the Acquisition Workforce to Rapidly Develop Capability; 3) Maximize Acquisition Flexibility through Reduced Regulations and Processes; 4) Develop High Performance Systems through Rigorous Enterprise Technical and Execution Excellence; and 5) Improve Effective Lifecycle Risk Management.

6.2	**UNITE! NATO and Ukraine align innovation efforts** The Ukraine-NATO Innovation, Technology, and Engineering (UNITE) program is the first joint NATO-Ukraine programme on scaling prototyped and tested innovative technologies that help meet interoperability requirements (source) *Assessment:* On 25 November, NATO announced the establishment of the UNITE - Brave NATO program to better align and accelerate defence innovation between the Alliance and Ukraine. Ukraine's defence tech cluster Brave1 will lead the effort from the Ukrainian side while NATO's Communications and Information Agency (NCIA) will lead NATO's contributions. The new entity's first activity will be a competition to bring new innovative counter unmanned aerial systems, air defence capabilities, and secure frontline communications, reflecting three priorities that have prominently featured in recent DEFTECH scan volumes. Teams of Allied and Ukrainian companies will compete for joint grants worth a total of €10 million allocated equally by NATO and Ukraine. Interested companies will be able to register online and are expected to be able to submit their bids in February 2026. Winners of the first UNITE-Brave NATO competition will be announced in spring 2026. The initiative is expected to scale to €50 million in total for 2026 with additional focus on signals intelligence systems, robust navigation in contested electromagnetic environments, and uncrewed ground vehicles.


deftech.ch