Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

deftech.scan

February 2023

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

https://deftech.ch/scans

deftech
defencefuturetechnologies

Dear Reader,

Considering the speed of the evolution and revolution in technology, the work of foresight with respect to long term i.e. 10+ years becomes increasingly challenging!

In order to cope with it, we are going to adopt, starting with the next release, a change of format as well as focus. Welcome therefore to the last version of this deftech.scan as it was structured during the last 12 months. You will realize how quickly science-fiction is becoming science-facts, merging simultaneously different generations of technologies.

1. ***Applications of AI and data*** **2**
2. ***Autonomous systems and robots*** **4**
3. ***Sensors*** **7**
4. ***Computing Power*** **8**
5. ***Connectivity*** **9**
6. ***Human Performance Enhancement and Protection*** **10**
7. ***New Weapons*** **11**
8. ***Space*** **14**

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	**LIGNex1 awarded deal to develop AI-based combat system for South Korean submarines** The $39.6 billion won ($30 million) contract marks the first time AI will be used in a combat system of a major South Korean military asset. (source and source) *Assessment:* The system is expected to manage several functions, including search and track, identification and classification of objects, tactical operations, and engagement, for either the KSS III or Dosan Ahn Changho-class submarine. LIGNex1 will work with the Korea Research Institute for Defense Technology, Planning, and Advancement (KRIT) as well as several academic partners. The contract is part of a more significant "Smart Navy" initiative that aims to more completely incorporate automation, AI, uncrewed systems, and human-machine teaming into the fleet. In December 2022, the ROK Navy announced a major reorganization that features the standing up of a Maritime Unmanned Forces Command and an ambitious effort to transform the fleet force structure. The RoK Navy is currently approximately 1% uncrewed. The plan seeks to transform the level of uncrewed assets to around 45% by 2045. The new Maritime Unmanned Forces Command will comprise of an uncrewed underwater flotilla, an uncrewed surface flotilla, and an uncrewed aerial fleet. According to Lee Jong-ho, ROKN Chief of Naval Operations "The Navy will create a mobile maritime three-axis force and pursue the development of advanced manned and unmanned systems based on artificial intelligence technology."

1.2	**Data, AI, and enhanced situational awareness in the Ukraine War** *The Washington Post* published two articles on "algorithmic warfare" in Ukraine on 19 and 20 December. The first piece describes how Ukraine is using data aggregation tools and machine learning processing of complex data sets to gain advantage over Russian forces. (source and source) *Assessment:* The article details how Ukraine's Armed Forces and NATO are using US-based Palantir's software platform to aggregate and process data—particularly commercial and military imagery and data from other battlefield sensors—and how fused and processed data is greatly enhancing situational awareness and targeting. According to the piece, "using a digital model of the battlefield, commanders can penetrate the notorious fog of war. By applying artificial intelligence to analyse sensor data, NATO advisers outside Ukraine can quickly answer the essential questions of combat: Where are the allied forces? Where is the enemy? Which weapons will be most effective against enemy positions?" Mykhailo Fedorov, Ukraine's minister of digital transformation, observed that this capability proved "especially useful during the liberation of Kherson, Izium, Khrarkiv, and Kyiv regions." The article also emphasizes the importance of the Starlink satellite network in providing broadband connectivity required to deliver information and intelligence along the command-and-control network. However, on 10 February, SpaceX's president and CEO Gwynne Shotwell announced the company will prevent Ukraine's military from using Starlink's service for controlling drones, surprisingly stating that the system "was never meant to be weaponized."

1.3	**Outfoxed by a box: US Marines demonstrate limitations of AI security camera** In his upcoming book *Four Battlegrounds: Power in the Age of Artificial Intelligence*, defence analyst Paul Scharre tells a story in which US Marines fooled US Army algorithms in creative and humorous ways, one of which may have drawn on tactics from a military-themed video game. (source and source) *Assessment:* The US Army asked a squad of Marines to help train AI security cameras being developed as part of the US Defense Advanced Research Projects Agency's Squad X program. After six days of training the algorithms by walking around in front of the cameras, the Marines were asked to try and defeat the AI in creative ways. Within a day, each of the eight Marines charged with testing the AI managed to traverse the 300 meter testing ground and touch the camera without being detected using creative techniques. Two Marines somersaulted across the ground while two others moved across the ground while hiding in a cardboard box—"giggling the whole way," according to an observer. The tactic may have been lifted from the military-themed video game *Metal Gear Solid* (see image below). Another Marine walked across the range dressed as a fir tree. DARPA deputy director Phil Root told Scharre that the Marines were able to avoid detection because the AI had only been trained to "detect humans walking, not humans somersaulting, hiding in a box, or disguised as a tree", even though most sentient humans would have easily discerned the Marines moving with a cardboard box over their head as a human threat. While amusing, the anecdote also underscores several emerging lessons about the development and use of defence and security applications of AI, including the brittleness of narrowly trained algorithms, the need for rigorous testing, and, perhaps most importantly, the importance of using machines to support human operators rather than replace them. As Scharre notes in his book: "an algorithm is brittle, . . . there will always be these edge cases . . .humans tend to have a much richer understanding of the world." Scharre's book is set to be released on 28 February.

Figure 1: A screen capture from a YouTube video showing a Metal Gear Solid game player using a cardboard box to sneak up on a fixed guard post manned by human operators. A similar tactic was used by US Marines to avoid detection by an AI security camera. Source: Kumikones YouTube channel

2. Autonomous systems and robots

2.1	**Iran building drone carrier ships** An image from November 2022 that circulated on social media in December and January 2023 shows the Iranian Revolutionary Guard Corps Navy refitting a commercial container ship to serve as a military vessel capable of carrying both rotary and fixed wing uncrewed aerial systems (UAS). (source) *Assessment:* *USNI News* Contributor HI Sutton published photos of the *Shahid Mahdavi* being refitted in late December. Sutton observed that the "conversion adds a large cantilever flight deck on the port side", much like the flight deck of a traditional aircraft carrier. However, "the fact that the superstructure spans the original deck means that a traditional aircraft carrier layout is not possible." Iran has a surplus of commercial cargo ships due to on-going sanctions and is expected to convert multiple commercial cargo ships to drone carriers. Previously, the Iranian Navy converted a former petrochemical tanker into the IRINS *Makran* forward base ship. That Iran is developing a drone carrier capability is not necessarily a surprise. Benham Ben Taleblu, an Iran expert with the Foundation for Defense of Democracies, observed that "Iranian media had talked about [the ship] being used to store drones to grow the long-range strike capabilities of the country." Additionally, in July 2022, the Iranian Navy announced the establishment of a "Drone carrier division." Like Turkey, whose drone carrier development efforts were detailed in the December 2022 DEFTECH scan, Iran has been active in the development of a range of uncrewed aerial systems (UAS), including the Shahed 136 loitering munition that has featured prominently in the conflict in Ukraine.

2.2	**US Navy orders two Kratos XQ-58A Valkyries for "killer drone project"** The US Navy has committed to operating the stealthy attritable aircraft as part of the service's secretive Penetrating Affordable Autonomous Collaborative Killer program. (source) *Assessment:* Kratos' Defense's Valkyrie was originally developed as part of the US Air Force's Low Cost Attritable Aircraft Technology (LCAAT) program and is among the most mature attritable / loyal wingman aircraft in the world. To date, the Valkyrie has been used as a technology demonstrated by the Air Force, though it is likely to be part of the sixth generation US Air Force Next Generation Air Dominance (NGAD) program. The Navy contract's total cost was $15.5 million dollars, which includes the production and delivery of the two aircraft as well as "sensor and weapons systems payloads." The Penetrating Affordable Autonomous Collaborative Killer program appears to be an approach to penetrate geographically dispersed anti-access / area denial systems that are likely to mark the future battlefield, especially in the Indo-Pacific. Low-cost autonomous uncrewed systems such as the Valkyrie operating in swarms or in conjunction with human operators could offer a lower-cost and lower-risk means of absorbing losses while still operating in contested airspace. The Valkyrie has a modular open architecture design to allow for rapid integration of multiple mission systems and software upgrades. The Navy's Valkyrie could carry intelligence, surveillance, and reconnaissance (ISR), communications, strike, or electronic warfare payloads.

2.3	**Turkey orders first uncrewed surface vessel (USV)** The Turkish Defence Agency (SSB) signed a contract in late December with Turkey based ARES Shipyard and Meteksan Defence to procure indigenously developed ULAQ USV. The deal involves the ULAQ anti-surface and anti-submarine variants. (source) *Assessment:* The ULAQ finished sea trials in January 2022 and has previously demonstrated its ability to carry four laser-guided Cirit missiles and two infrared-guided L-UMTAS missiles. However, in December 2022, the SSB announced a new ULAQ configuration with enhanced interoperability with drones and other unmanned platforms to facilitate cross-domain uncrewed naval operations. The reportedly upgraded ULAQ is also now equipped with a new, locally made propulsion system that will increase its speed. Other upgrades associated with the new configuration include: 1) a llight, durable, and proven composite hull, 2) active and passive stabilization systems, 3) improved seaworthiness in tough sea conditions, 4) enhanced vision and driving abilities with LIDAR, 5) wide-angle navigation camera, radar, and EO/IR camera, 6) an AKSON C-Band Data link and swarm communication, 7) satellite communication, 8) precise maneuverability in littoral waters, 9) full autonomy with image processing and sensor fusion, and 10) stationary and mobile control station options. The ULAQ has an advertised range of 400 km and maximum speed of 65 km/h. While Turkey has become one of the world's leading developers and exporters of UAS, the ULAQ is the country's first indigenously developed USV. The ULAQs are expected to enter service "in the following months."

Figure 3: Screenshots of the ULAQ USV taken from an SSB / Meteksasn Defence Video.

2.4	**Duct tape and ingenuity: make-shift drones on the battlefield in Ukraine** Both Ukrainian and Russian forces have employed make-shift drones to carry out both intelligence, surveillance, and reconnaissance (ISR) and strike missions. (source) *Assessment:* A video posted on Telegram shows an improvised fixed-wing drone held together by duct tape that the Ukrainian Sonechko unit has employed in strike missions against Russian forces. The exceptionally inexpensive drone is made of "foam plastic, mounting foam and Chinese spare parts" and is held together by duct tape. The drone reportedly was armed with a 1.3kg RKG-3 anti-tank grenade, though the video also shows Ukrainian forces assembling anti-personnel fragmentation bombs by packing plastic explosives into pipes and wrapping a layer of ball bearings around them with plastic film and tape. Ukraine is not alone in leveraging the ingenuity of its soldiers to build cheap, expendable, but effective, drones. Sam Bendett, a Russian military expert with the CNA Corporation and Center for a New American Security (CNAS) observed that "Russia has a lot of volunteer efforts building small quadcopters and other small UAVs", citing an example of how state media had "praised soldiers for putting together their own ISR quadcopter." Still, Bendett assesses that Russia's volunteer make-shift drone production efforts are playing catch-up as they are "probably still smaller in scale and some of these efforts started later than their Ukrainian counterparts."

Figure 4: An image of a homemade drone used by the Sonechko against Russian forces in Ukraine. source: Sonechko Volunteer Battalion via Telegram as published by Forbes

3. Sensors

3.1	**New application for Thales sonar could expand both capability and risks** The US Navy confirmed it has procured Thales' CAPTAS – 4 variable depth sonar as part of its FFG-62 Constellation class frigate program. In January, Thales representatives demonstrated the CAPTAS-4 could be rapidly installed on a commercial vessel, potentially greatly expanding the US submarine hunting capability. (source and source) *Assessment:* The Navy selected the system after moving away from plans to use Raytheon's Dual-mode Array Transmitter (DART) due to persistent concerns over technical risk. A total of 10 CAPTAS-4 systems are set to be ordered. The CAPTAS-4 is already in service in France, Italy, Morocco, Egypt, Greece, the UK and Chile. During the Surface Navy Association conference in Arlington, Virginia in January, Thales representatives showed a video of the system being installed on a commercial ship within a 48-hour time period. Enlisting commercial vessel to support the anti-submarine mission could serve as a valuable force multiplier if conversion from commercial to military asset can happen rapidly, allowing the navy to respond more effectively to fast moving crises. In addition to outfitting commercial ships with intelligence, surveillance, and reconnaissance (ISR) equipment, many militaries have pursued containerized missile systems in which missiles are transported stealthily and then launched from items that look like traditional shipping containers. Russia's Rosoboronexport, for example, has developed the Club-K container missile system. Of course, placing military sensors—much less weapons—on board commercial ships raises questions of the status of these ships, likely raising the risks of shipping and other commercial vessels being considered legitimate military targets under certain circumstances.

3.2	**New radar for F-35 but questions remain about its capabilities** The Block 4 upgrade of all three variants of the F-35 will include integration of a new radar to "provide unparalleled battlespace situational awareness" and "help ensure air superiority", according to Northrop Grumman, the radar's manufacturer. (source and source) *Assessment:* The US Department of Defense confirmed in January that the F-35 Block 4 upgrades will involve a new radar designated the AN/APG-85. The F-35 currently is equipped with the Northrop Grumman AN/APG-81. Little is known about enhanced capabilities the AN/APG-85 will enable, despite media queries to both the US DoD and Northrop Grumman, as discussed in a recent Aviation Week podcast on the future of the F-35.*The Drive* speculates that "a Gallium Nitride (GaN)-based system is very likely to be a major facet of this improvement, which could drastically increase the F-35's radar range and resolution." Improved ability to support electronic warfare tactics was also cited as likely being a "key factor." In a January 11 press release Northrop Grumman stated that the "AN/APG-85 is an advanced multifunction sensor that will be compatible with all variants of the F-35 aircraft and will be capable of defeating current and projected adversarial air and surface threats. The development and integration of APG-85 will incorporate some of the latest technologies available and help ensure air superiority." The AN-APG/85 is part of a much more extensive set of upgrades set for Block 4 development also likely to include an upgrade of the fighter's computing system, electro-optical targeting system, distributed aperture system, and electronic warfare suite.

4. Computing Power

4.1	**Chinese researchers claim to discover way to break encryption using quantum computers** A group of 24 Chinese researchers published a paper in which they claim to have devised a means to use a quantum computer with only 372 qubits to break the widely used 2048-bit RSA encryption algorithm. Observers have expressed doubt that the paper's approach could be scaled to break the most sophisticated versions of RSA encryption. (original paper and source and source) *Assessment:* The paper was jarring for computer security analysts who worry that its findings could indicate a greatly shortened timeline for breaking the widely used RSA algorithm, especially given that 372 qubit quantum computers are almost within reach today. For example, IBM's Osprey system, which is expected to be commercially available in 2023, is advertised as having 433 qubits. Computer security expert and author Roger Grimes noted to the *Financial Times* that "it's a huge claim. It would mean that governments could crack other governments secrets. If it's true—a big if—it would be a secret like out of the movies, and one of the biggest things ever in computer science." However, many experts and observers believe significant caveats and scepticism should accompany the research. This scepticism is rooted in doubt over the ability of the Chinese researchers to scale the findings from a much less ambitious experiment. The experiment carried out by the researchers involved using a hybrid technique that combined a 10 qubit quantum computer with traditional computing methods to break a less secure 48-bit RSA encryption algorithm. The Chinese researcher's assertion is that they could do the same to the more advanced 2048-bit RSA algorithm that uses much larger prime numbers as the basis of its encryption if they had access to a more powerful 372-qubit computer. Quantum computing scientist Peter Shor believes the paper may be conceptually correct, but that it did not adequately address "how fast the algorithm will run" and suggests that "it may take millions of years" to break 2048-bit RSA. Even the research team acknowledges ambiguity about the pace of encryption breaking, writing that the "quantum speed-up of the (encryption breaking) algorithm is unclear." One quantum computing expert described the overall claim of being able to break advanced RSA encryption as "like someone claiming he's found a way to land a spaceship on the moon because he built a rocket in his backyard that jumped the fence into his neighbour's yard." Nonetheless, the paper should not be summarily dismissed. It, and the intense discussion around it, demonstrate both the gathering pace of development of quantum computing as well as the potentially highly-disruptive effects this accelerating development may have on government, commercial, and private communications.

5. Connectivity

5.1	**Japan to expand and extend cyber-defence capability** Japan has taken multiple steps to expand and extend its cyber-defence capabilities in response to increasing cyber threats from China and North Korea (source and source) *Assessment*: Japan's maturing appreciation of the threat to national security stemming from China and North Korea's cyber activities spurred two announcements designed to increase national cyber-defence and resilience in the reporting period. In January, Japan's Ministry of Defence announced that the Japan Self Defence Force would quadruple the size of its cyber-defence force from 890 today to nearly 4,000 in four years. While this constitutes an impressive and necessary increase, this number is far fewer than the estimated 175,000 cyberwarfare personnel in China's People's Liberation Army (PLA) and even the 7,000 cyber-warriors in North Korean's military. Concern over growing cyber threats has also led the Japanese government to develop a legal and process framework that will allow the JSDF's cyber-defence unit to protect private sector businesses and critical infrastructure networks. The expectation is that new frameworks for allowing the JSDF to help protect private companies will be established in 2024. The first implementation step will be to establish a system for protecting Japan's defence industry by 2027 with support being extended to operators of critical infrastructure in 2028 and beyond.

5.2	**Oops, they did it again: sensitive information released in on-line game chat** Sensitive information about the F-16A Fighting Falcon and the F-15E Strike Eagle was posted in the messaging forum of massive multiplayer online game *War Thunder* on 17 - 18 January. (source and source) *Assessment*: *War of Thunder* is a free game that allows players to do combat against one another in highly-realistic operational and tactical environments. Game players have previously published sensitive or even classified information to win on-line arguments or demonstrate to the game's designers that models are innacurate. A previous DEFTECH scan volume documented how classified information on British and French tanks and a Chinese anti-tank weapon have been posted without authorization. In the latest incidents, a user posted information about the F-16A Fighting Falcon and, then, the day after, a second user posted sensitive information on the F-15E. The first leak involved a post of a F-16A manual that detailed how the aircraft would equip the AIM 120 Advanced Medium Range Air to Air Missile (AMRAAM). The F-16A is the oldest model of the F-16 family and has been extensively upgraded since the first A-variant was delivered in 1979. The individual that shared the information reportedly believed it was so old as to not violate sharing rules. However, the game's owners at Gaijin Entertainment took the post down as it did violate the US International Trafficking in Arms Regulation (ITAR). On 18 January 2023, a user posted numerous Operational Flight Program (OFP) software manuals from 1998- 2000 for the F-15E, including ones on flight controls, navigation, targeting, and weapons systems. To many these stories seem to be harmless, however, they do reveal the growing ways in which the digital and physical worlds are intersecting and interacting with potentially important implications for defence and security communities.

6. Human Performance Enhancement and Protection

6.1	**Patriot games: Ukrainian troops head to Oklahoma for expedited training on Patriot missile systems** A hundred Ukrainian soldiers have begun a compressed training course on Patriot missile defence systems at a training facility in Fort Sill, Oklahoma. (source) *Assessment:* The typical Patriot training program is two-years, though this program will be shortened considerably to expedite the timeline for the use of the Patriot system in the on-going conflict in Ukraine. The US Air Force trainers are confident the shortened timeline will not require sacrificing structure, rigor, or quality. According to US Air Force Brigadier General Pat Ryder, "we're not winging it in terms of the training. This will be an established curriculum to train the soldiers on the Patriot system." In addition, the Ukrainians selected for training in Oklahoma have a background in and familiarity with air defence artillery equipment and concepts, which is expected to help increase the pace of adoption of training. Also in January, the US began its training of 500 Ukrainian forces in combined arms at the Grafenwoehr training area in Germany with the goal of having the Ukrainian forces returned to the front lines within five to eight weeks. Pentagon press secretary, US Air Force Brigadier General Pat Ryder, said the training is designed to "give [Ukrainian forces] this advanced level of collective training that enables them to conduct effective combined arms operations and manoeuvre on the battlefield. The training will include classroom instruction and field work.

6.2	**The cloud, space, and global models: trends in military training and simulation for 2023** *Shephard Media* published an exclusive interview with Bohemia Interactive Simulations' chief commercial officer Peter Morrison in January in which he identified four high-level trends for virtual training solutions in 2023. (source) *Assessment:* Beyond confirming growing demand for virtual and augmented reality head-mounted displays and high-fidelity, whole-Earth terrain enterprise systems, Morrison also identified four broader trends shaping the future of virtual military training and simulation. First, militaries are seeking to scale access to virtual / augmented training solutions by allowing software to run in the cloud. Morrison cited his own company's VBS software, which has always run as a Windows application, "but it's limited in terms of scale" to 2,000 to 3,000 entities. By running a scalability architecture on the cloud, the system could potentially handle tens or hundreds of thousands of users without a loss in quality. Second, there will be a growing interest in space-focused simulations as both military and commercial interest and activity in space increase. Third, there is also a growing desire to better aggregate data from training and simulations so that it can be effectively processed by machine learning. This will speed up and improve the ability of operators to gain more precise lessons about training exercises and simulations. It will also help organizations develop individualized training curriculum. Finally, Morrison highlighted a need for more ambitious simulation capabilities that capture the increasing complexity and intricate dependencies of the future fight. According to Morrison some customers are asking for "a version of Planet Earth, a digital twin, where large-scale ongoing conflict can be simulated, including the effect on the civilian population and the effect on terrain."

7. New Weapons

7.1	**"It's a bird, it's a plane, it's . . . a high-altitude spy balloon": Chinese spy balloon shot down after bizarre four-day incursion over US territory** The incident reveals a years-long global effort by China to use high-altitude balloons for surveillance. (source and source) *Assessment:* The incursion into US airspace was the fifth by a high-altitude balloon over the last several years, though previous incursions were not recognized as Chinese spy balloons at the time. Data collected during these previous episodes allowed the US Northern Command to identify the balloon and track it as it made its slow-motion trip across the United States, flying at around 60,000 feet. The balloon was publicly spotted on 30 January over Air Force intercontinental ballistic missile fields in Montana. The US Department of Defense noted that measures were taken to ensure the balloon did not collect intelligence while on its journey. It was subsequently shot down by an F-22 using an AIM-9 sidewinder missile on 4 February over US territorial waters off the Atlantic Ocean coast of South Carolina. The F-22 fired the AIM-9 at 58,000 feet, and the missile intercepted the balloon at between 60,000 and 65,000 feet. Early reports gathered from the wreckage of the balloon indicate it had tools to monitor US communications. According to *Aviation Week,* the incident has revealed several interesting insights. First, it showed the capability of an F-22 to shoot down an aircraft at exceptionally high altitudes, a task that was not assured given the low radar and heat signatures of the balloon. Moreover, AIM-9s have never been tested at the altitude at which they were employed. Second, the design of the balloon and use of opaque, rather than translucent fabric, appears to be a significant step forward in high-altitude balloon technology. The opaque material appears to have been able to reflect the sun's energy rather than letting it pass through, creating a more efficient system to regulate temperature without adding too much structural weight. Three additional unknown and unauthorized objects were shot down over US and Canadian territory between 5 – 12 February. The increase in air intercepts over North America is conspicuous, though also at least partially explainable. Radars use filter parameters to ensure that they are able to discern between signal—or items that need to be tracked—and noise—the large amounts of items in the air that are unlikely to be threats or warrant tracking. The North American Aerospace Defense Command (NORAD) had long filtered out size and speed profiles consistent with the Chinese spy balloon. After expanding the filters to include slower flying vessels, NORAD radars have located a number of other items that have been determined to pose a threat to US and Canadian national security and civilian air traffic.

7.2	**Blinded by the light—literally: China's coast guard uses laser against Philippine coast guard vessel** On February 13, the Philippine coast guard announced one of its vessels had been hit with "a military-grade laser light" that temporarily blinded crew members on the bridge. (source) *Assessment:* The Philippine vessel was escorting a resupply ship supporting forces stationed on Second Thomas Shoal, a submerged reef in the South China Sea that is part of the Philippines. China also claims the shoal. The Philippines intentionally grounded the navy sentry ship BRP Sierra Madre on the shoal in 1999 and the ship has been maintained by a contingent of Philippine Marines ever sense. In an effort to block the resupply of the Philippine Marines, the Chinese coast guard ship illuminated the laser twice toward the BRP Malapascua, "causing temporary blindness to her crew at the bridge," according to the Philippine coast guard. The Chinese coast guard ship also maneuvered to within 137 meters of the Philippine vessel. The Philippine coast guard decried the provocation in a statement, noting that "the deliberate blocking of the Philippine government to deliver food and supplies to our military personnel on board the BRP Sierra Madre is a blatant disregard for, and clear violation of, Philippine sovereign rights." Beyond the geopolitical implications, though, the incident also demonstrates the operational use of directed energy weapons beyond the much publicised roles of counter-drone and cruise missile defence to achieve less than lethal effects.

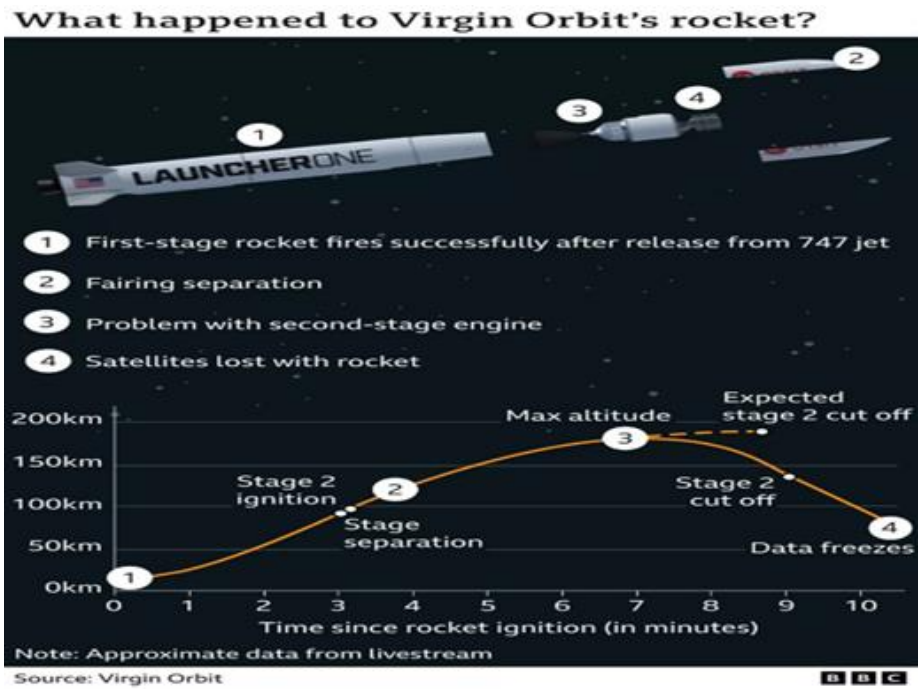
7.3	**Tempest and F-X unite: introducing the Global Combat Air Programme (GCAP)** The United Kingdom, Italy, and Japan have agreed to consolidate sixth generation fighter programs in an effort to share costs and technology, support local defence industrial bases, and build a potential larger international development program. (source) *Assessment:* The United Kingdom, Italy, and Japan have agreed to work together to develop a sixth-generation fighter jet with the ambition to produce a system able to fly by 2035. The GCAP programme appears to merge Japan's F-X future fighter program and the United Kingdom-led Tempest program, which was being pursued in conjunction with Italy. While developing the capability to meet a more challenging external security environment is at the core of the program, GCAP is also designed to boost each country's domestic defence industry. A UK Ministry of Defence announcement emphasised that "the project is expected to create high-skilled jobs in all three countries, strengthening our industrial base and driving innovation with benefits beyond pure military use." The first phase of the project will include developing an agreement on cost-sharing, establishing the core platform concept, and setting up the structures needed to deliver the project. The program may also be open to additional international partners.

7.4	**Doomsday clock keeps ticking: Russia produces first nuclear warheads for Poseidon torpedo** On 16 January, Russian state news agency *Tass* reported that the first nuclear ammunition loads have been manufactured. (source and source) *Assessment:* Originally announced in 2018, the Poseidon is billed as an unstoppable nuclear-powered, nuclear-armed torpedo with essentially unlimited range. The "super weapon" is designed to travel at up to 80mph deep underwater and carry a two-megaton (2,000 kilotons) nuclear warhead. While the report does indicate a step forward for the Poseidon weapons system, it comes on the heels of a likely setback. In November 2022, several international media sources reported that a scheduled test of the Poseidon was scrubbed due to technical difficulties. The reports were based on sources in the United States intelligence community that indicated the Belgorod submarine on which the Poseidon was to be tested returned to port without any evidence of the test having taken place.

7.5	**Israeli company Regulus Cyber introduces new C-UAS system** The Ring R1 C-UAS system uses global navigation satellite system (GNSS) manipulation to enable the user to take control of individual drones or drone swarms (source, source, and source) *Assessment:* In a press release issued on 19 January, the company introduced its Ring R1 C-UAS system that uses advanced spoofing technology to hijack and manipulate feeds from GNSSs such as GPS, GLONASS, Galileo, and BeiDou. The system is comprised of a transmitting antenna, a GNSS receiving antenna, and the Ring Effector. The company's product page and promotional video stress the flexibility of use of the system in meeting a range of threats, including threats from drone swarms, as well as the ease of set up, integration with other C-UAS solutions, and use. An operator can select different modes to achieve different interdiction effects ranging from keeping the UAS in a holding pattern, diverting the UAS, forcing landings, or destroying the drone by crashing it into the ground. According to Yonatan Zur, company CEO, Regulus "have successfully tested the system against over 45 different types of UAS, rotary- and fixed-wing." The company also stresses that the system is "fully operational and combat proven" and that it has "already been selected by Police, HLS and Defence forces around the world for both tactical deployments and for strategic locations." To this end, an online promotional video depicts the system defending a nuclear plant from a drone swarm attack.

8. Space

8.1	**UK misses out on historic first after failed satellite launch with defence payloads** A Virgin Orbit launch rocket carrying several small satellites, including military satellites, failed to achieve a planned orbit on 10 January. If successful, the launch would have marked the first time a Western European nation had placed satellites in space from a base on home soil. (source and source) *Assessment:* The two-stage rocket was launched from under the wing of a modified Boeing 747 that had taken off from the runway at Spaceport Cornwall in Newquay in southwest England. However, an unexplained anomaly occurred during the firing of the rocket's second stage engine leading to the rocket missing the required orbit. The Virgin Orbit was carrying several small satellites with military-related payloads, including: • Two of the UK government's Prometheus 2 satellites, which were planned to operate in Low Earth Orbit (LEO) and test imaging and monitoring of radio signals • A joint US Naval Research Lab / UK Defence Science and Technology Laboratory (DSTL) cubesat that was part of the two organizations' collaboration on the Circe program that involves investigating the ionosphere • Amber 1, a UK defence satellite designed for maritime intelligence gathering. The satellite that was lost with the failed launch was expected to be the first of 20 or more satellites to improve maritime domain awareness The UK space community saw the failed launch as a disappointment but also as only a temporary setback as the country seeks to enter the market of satellite launch services. Ian Annett, Deputy CEO of the UK Space Agency, predicted further launches in the next 12 months and observed that the launch "is still an immense moment of national pride … we go back, we get up, we do it again, and that defines our future." Adam Baker, a space industry consultant quoted in *BBC* reporting, agreed with Annett's assessment, noting that "this is just the start of a much longer commercial spaceflight journey that the UK is only just starting to make."




https://deftech.ch/